MASTER SERVICES AGREEMENT

between

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, AS REPRESENTED BY THE MINISTER OF LABOUR AND CITIZENS' SERVICES

and

EDS ADVANCED SOLUTIONS INC.

as of March 30, 2009

MASTER SERVICES AGREEMENT

TABLE OF CONTENTS

THIS MASTER SERVICES AGREEMENT is entered into as of March 30, 2009 (the "**Effective Date**"), between **EDS Advanced Solutions Inc.** (the "**Service Provider**"), a company incorporated under the laws of British Columbia and **Her Majesty the Queen in Right of the Province of British Columbia as represented by the Minister of Labour and Citizens' Services** (the "**Province**").

RECITALS

A. The Province conducted a competitive procurement process under the JSRFP for purposes of establishing a contractual business alliance with an experienced and qualified third party to, among other things, provide strategic transformation and mainframe services to the Province and the Broader Public Sector;

B. As a result of the JSRFP process, the Province selected EDS Canada to provide certain services through the Service Provider to the Province and the Broader Public Sector, subject to, and in accordance with, the terms of this Agreement;

C. The Service Provider is Corporately Controlled by EDS Canada and EDS Canada is an Affiliate of the Corporate Guarantor;

D. EDS Canada caused the Service Provider to enter into this Agreement with the Province regarding the provision of such services to the Province and the Broader Public Sector;

E. EDS Canada has agreed to grant a guarantee in favour of the Province, for the performance of the obligations of EDS under this Agreement, and to cause the Corporate Guarantor to grant a guarantee, in favour of the Province, in respect of certain obligations of EDS under this Agreement; and

F. Every member of the Broader Public Sector who wishes to acquire services from EDS under the Province's competitive procurement process will enter into a separate services agreement in the form attached as Appendix B to **Schedule 26** (*Growth and Marketing*) (each a BPS Services Agreement), and in accordance with the terms and conditions of this Agreement, as applicable;

G. The Parties are dedicated to the security of information and protection of privacy and Personal Information, and have therefore structured this Agreement, and the relationship between the Parties, in order to ensure that the same is achieved.

IN CONSIDERATION of the foregoing and the mutual covenants and agreements contained in this Agreement, the Parties covenant and agree as follows:

ARTICLE 1 – INTERPRETATION AND GENERAL MATTERS

1.1 Definitions.

Unless otherwise provided in this Agreement (or in any Schedules attached to this Agreement), capitalized terms will have the meanings given to those terms in the attached **Schedule 1** *(Definitions)*. In addition to the definitions contained in **Schedule 1** *(Definitions)*, any capitalized terms defined elsewhere in this Agreement will have the meanings so given to them.

1.2 Recitals.

The recitals to this Agreement are intended to be a general introduction to this Agreement and are not intended to expand the scope of the Parties' obligations under this Agreement or to alter the plain meaning of the terms and conditions of this Agreement.

1.3 Headings.

The division of this Agreement into Articles, Sections, Subsections, paragraphs and clauses, and the insertion of headings, are for convenience of reference only and will not affect the construction or interpretation of this Agreement.

1.4 Interpretation.

In this Agreement, unless expressly stated to the contrary:

(a) the terms "this Agreement", "the Agreement", "hereof", "hereunder", "hereto" and similar expressions refer, unless otherwise specified, to this Agreement taken as a whole and not to any particular Article, Section, Subsection, paragraph, clause or other portion of this Agreement;

(b) words importing the singular number only will include the plural, and vice versa, and words importing gender will include all genders;

(c) unless something in the subject matter or context is inconsistent therewith, all references in this Agreement to Articles, Sections, Subsections, paragraphs, clauses and Schedules refer to Articles, Sections, Subsections, paragraphs, clauses and Schedules of this Agreement;

(d) words and phrases denoting inclusiveness (such as "including" or "includes"), whether or not stated as being without limitation, are not limited by their context or the words or phrases which precede or succeed them;

(e) unless otherwise provided in this Agreement, whenever the words "discretion", "option", "determine", "election" and other similar words or any variations thereof are used with respect to a Party, they will be deemed to mean such Party's sole and absolute discretion, option, determination, election or other such similar act;

(f) any reference to a statute will be deemed to refer to the statute and any regulations made thereunder in force as at the date hereof, as the same may be subsequently amended, expanded, added-to, supplemented or otherwise changed or replaced from time to time, unless otherwise expressly provided in this Agreement; and

(g) unless specifically provided otherwise in this Agreement, any reference to "knowledge" of the Service Provider or any officer or other personnel of the Service Provider means the knowledge of the Service Provider after having made due enquiry, and if the Service Provider fails to make such due enquiry, then the knowledge that the Service Provider would have had if the Service Provider had conducted reasonable enquiry into the subject matter.

1.5 Acting Reasonably.

With respect to the Service Provider, any requirement set forth in this Agreement for the Service Provider to act reasonably, use reasonable efforts, or any variations thereof, will mean the use of all reasonable commercial efforts having regard to the surrounding circumstances, unless specifically provided otherwise. With respect to the Province, any requirement set forth in this Agreement for the Province to act reasonably, use reasonable efforts, or any variations thereof (including, without limitation, any requirement for Approvals by the Province not to be unreasonably withheld), will not require the Province

to act in a manner that is contrary to, or is inconsistent with, any other policies, directives, executive directions, Treasury Board decisions, guidelines, rules, regulations, legislation or other determinations of the Province. In addition, the Service Provider expressly acknowledges and confirms that nothing contained in this Agreement will be construed or otherwise interpreted in any manner that would or could cause the Province to fetter its discretion.

1.6 Accounting Policy.

In this Agreement all references to "**GAAP**" refer, unless otherwise specified, to generally accepted accounting principles from time to time approved by the Canadian Institute of Chartered Accountants (or any applicable successor institute thereto) as at the date on which such calculation is made or required to be made, consistently applied. Unless otherwise provided in this Agreement, all accounting, record keeping, book keeping and other actions of the Service Provider contemplated in this Agreement will be performed and carried out in a manner that is consistent with GAAP.

1.7 Calculation of Time Periods.

Unless otherwise specified in this Agreement, when calculating the period of time within or following which any act is to be done or any step taken, the date that is the reference date for starting the calculation of such period will be excluded and the final date for completing such act or step will be included.

1.8 Currency References.

Unless otherwise specified, all dollar references in this Agreement are deemed to refer to lawful money of Canada.

1.9 Time.

Time will be of the essence of this Agreement.

1.10 Schedules.

The following are the Schedules attached to this Agreement, which are incorporated into this Agreement by reference and are deemed to be an integral part of this Agreement:

Schedule 1 - Definitions
Schedule 2 - Transition Plan
Schedule 3 - Transition Management and Governance
Schedule 4 - Work-in-Progress Projects
Schedule 5 - Special Terms
Schedule 6 - Basic Services
Schedule 7 - Language of Services
Schedule 8 - Service Locations
Schedule 9 - Transformation
Schedule 10 - Transformation Plan
Schedule 11 - Service Levels
Schedule 12 - Service Level Failures
Schedule 13 - Changes to Weightings
Schedule 14 - Non-Disclosure Agreement
Schedule 15 - Conditions of Use of Province Marks
Schedule 16 - Province Marks
Schedule 17 - Communications Plan and Processes

Schedule 18 - Governance
Schedule 19 - Key Positions
Schedule 20 - Subcontractor Matters
Schedule 21 - Reporting Requirements
Schedule 22 - Records Protocols
Schedule 23 - Fees
Schedule 24 - Privacy Obligations
Schedule 25 - Corporate Chart
Schedule 26 - Growth and Marketing
Schedule 27 - Gainsharing
Schedule 28 - Specific Laws and Policies
Schedule 29 - Additional Representations and Warranties
Schedule 30 - Indemnification Matters
Schedule 31 - Limitation on Liability
Schedule 33 - Performance Guarantee
Schedule 33 - Corporate Guarantee
Schedule 34 - Insurance
Schedule 35 - Form of Insurance Certificate
Schedule 36 - Material Breach
Schedule 37 - Remedies for Material Breach
Schedule 38 - Termination Fees
Schedule 39 - Service Provider Code of Conduct
Schedule 40 - JSRFP
Schedule 41 - Province Shared Infrastructure
Schedule 42 - Designated Arbitrators
Schedule 43 - Software Responsibility Table

1.11 Document Conflicts.

The main body of this Agreement, the Schedules attached to this Agreement, the Transaction Documents and the JSD Agreement are to be interpreted so that all of the provisions are given as full effect as possible. In the event of a conflict among the foregoing, and unless expressly stated to the contrary, the order of precedence will be as follows:

(a) first, the main body of this Agreement;

(b) second, any Schedules attached to this Agreement provided that **Schedule 1** (*Definitions*), **Schedule 5** (*Special Terms*), **Schedule 24** (*Privacy Obligations*), **Schedule 6** (*Basic Services*), **Schedule 11** (*Service Levels*), **Section 12** (*Service Level Failures*), **Schedule 20** (*Subcontractor Matters*), **Schedule 23** (*Fees*), **Schedule 38** (Termination Fees), **Schedule 31** (*Limitation on Liability*) and **Schedule 37** (*Remedies for Material Breach*) shall take precedence over the other Schedules to this Agreement;;

(c) third, any other Transaction Documents; and

(d) fourth, the JSD Agreement.

1.12 Joint Drafting.

The Parties have jointly contributed to the drafting of this Agreement, the Schedules attached to this Agreement and the Transaction Documents. Accordingly, it is the intention of the Parties that the

principle of *contra proferentem* will not apply with respect to interpretation matters in respect of this Agreement or the other Transaction Documents.

1.13 Objectives of the Parties.

The Parties acknowledge and agree that the primary objectives and guiding principles of their contractual relationship under this Agreement are as follows:

(a) for the Service Provider to transition and deliver data hosting services (including mainframe services), data centre facility services and a transformation strategy to realize the Parties objectives, as well as other additional services set forth in or contemplated by this Agreement;

(b) to identify strategic transformation opportunities that will address business challenges and operational risks associated with data hosting services and data centre facility services, that align with the long term business objectives of government, including the government's goals for environmental sustainability, and the Broader Public Sector and transform the current service delivery structure to meet the future needs of government and the Broader Public Sector;

(c) to achieve the technical objectives established (e.g., infrastructure technology operated 24 X 7, 365 days a year while meeting or exceeding the service delivery requirements and service levels);

(d) to achieve the objectives within the financial parameters agreed to by the Parties including a scalable utility pricing model;

(e) to develop a long term and mutually beneficial business relationship characterized by, among other things, mutual cooperation, good faith and flexibility to allow for the addition or removal of services within the scope of the Services described in (and in accordance with) this Agreement, as well as the flexibility to make such adjustment to the Services as may be necessary or otherwise required as a result of any unforeseen conditions or circumstances;

(f) to allow the Service Provider to meet or exceed the Province's service delivery requirements and service levels as described in this Agreement with respect to the Services, and where possible, to continually seek improvement in the delivery of all aspects of the Services;

(g) to develop sufficient business processes to accommodate volume fluctuations inherent in the nature of the Services being delivered;

(h) to have the Service Provider act as a source of "best practices" for the Province by having the Service Provider (and its Affiliates) monitor and evaluate changes and trends in the data hosting services (including mainframe services) and data centre facility services field (including an evaluation of related available and emerging technologies and services), and to so inform the Province in respect thereof from time to time;

(i) to protect the security and privacy of the Personal Information of the Province so that there is no material risk that any such information:

(i) will be disclosed or used contrary to the terms of this Agreement or any Applicable Laws, or

(ii) exists, is stored or can otherwise be accessed anywhere other than in British Columbia (or elsewhere in Canada as may be permitted under or pursuant to this Agreement), whether in its original form or otherwise, without the Approval of the Province;

(j) to minimize any adverse impact on the applicable personnel and business operations of the Province by effectively structuring and managing the transition of the responsibility for the delivery of the Services to the Service Provider;

(k) to enable the Service Provider to perform the Services at a high level of service, efficiency and effectiveness (and to avoid the operational management of the Services by the Province);

(l) to establish and maintain a fair economic business arrangement for both Parties during the Term; and

(m) to provide for the transition of the Services (other than the Termination Services) to the Province or the Alternative Service Provider upon the expiry or earlier termination of this Agreement in a manner that is efficient, enables continued and uninterrupted delivery of such Services during each such transition, and minimizes any adverse impact on the businesses of the Province in connection therewith.

The Parties acknowledge and agree that the above noted objectives and guiding principles are not, as such, intended to create legal obligations for the Parties, but instead, are intended to document the mutual primary objectives of the Parties in entering into this Agreement. The specific provisions of this Agreement and the other Transaction Documents are to be interpreted according to their plain meaning; provided that where there is uncertainty concerning the meaning of any specific provision, then such provision is to be interpreted in light of the objectives and guiding principles set forth in this Section.

1.14 General Scope.

The scope of the Services for the Term of this Agreement is as follows:

(a) the Services described as being in-scope for this Agreement in the provisions of this Agreement (and any Schedules attached to this Agreement); and

(b) the potential scope of the services set forth in the JSRFP including, without limitation, any potential scope, future scope or other similarly described scope in the JSRFP, subject to the implementation of such services at the discretion of the Province in accordance with the Change Order Process and other applicable terms of this Agreement.

The Parties acknowledge that it is their intention to expand the Services throughout the Term within the potential scope of services for this Agreement, as set forth above. Notwithstanding the foregoing, the Service Provider acknowledges and agrees that any additional services that are within such potential scope are subject to negotiation (to the extent applicable) and incorporation into this Agreement through the Change Order Process, by a written instrument signed by the Parties, or as may otherwise be specifically provided for under the terms of this Agreement. The reference to such potential scope in this Section or elsewhere in this Agreement does not, in and of itself, give the Service Provider any automatic or implied right to negotiate, discuss, or incorporate any additional services under this Agreement within

such potential scope, and such negotiations, discussions or incorporation will be at the sole discretion of the Province.

ARTICLE 2 – AGREEMENT TERM AND RENEWAL

2.1 Initial Term of the Agreement.

The "**Initial Term**" of this Agreement will commence on the date of this Agreement and will continue until the earlier of:

(a) the date upon which this Agreement is terminated in accordance with the provisions of this Agreement; or

(b) March 31, 2024.

The Initial Term may be extended in accordance with Section 2.5 (*Renewal Option*) and Section 2.8 (*One Year Extension*).

2.2 Initial Term of the Services.

Notwithstanding the provisions of Section 2.1 (*Initial Term of the Agreement*), within the Initial Term of the Agreement there are specific service delivery terms for the Data Centre Services and the Managed Services as follows:

(a) the initial term for the Data Centre Services ("**Initial Term DC Services**") will commence on the date of this Agreement and will continue until the earlier of:

(i) the date upon which this Agreement is terminated in accordance with the provisions of this Agreement; or

(ii) March 31, 2024; and

(b) the initial term of the Managed Services ("**Initial Term Managed Services**") will commence on the date of this Agreement and will continue until the earlier of:

(i) the date upon which this Agreement is terminated in accordance with the provisions of this Agreement; or

(ii) March 31, 2021.

Each of the Initial Term DC Services and the Initial Term Managed Services may be separately renewed in accordance with Section 2.5 (*Renewal Option*) and may be separately extended in accordance with Section 2.8 (*One Year Extension*);

2.3 No Renewal Assurances.

The Province is giving no assurances whatsoever to the Service Provider, expressed or implied, that this Agreement, or the Data Centre Services or Managed Services, will be renewed or extended beyond the expiry of the Initial Term or the Initial Term DC Services or Initial Term Managed Services, as the case may be. The Service Provider specifically acknowledges and affirms that it has arranged its business affairs on the assumption that:

(a) this Agreement will terminate at the end of the Initial Term;

(b) the Data Centre Services will terminate at the end of the Initial Term DC Services; and

(c) the Managed Services will terminate at the end of the Initial Term Managed Services,

and the Service Provider acknowledges that this Agreement, the Data Centre Services and the Managed Services may terminate prior to the Initial Term, the Initial Term DC Services, and the Initial Term Managed Services, respectively, in accordance with the provisions of Article 28 (*Default and Termination*).

2.4 No Expropriation.

Any termination of this Agreement in accordance with its terms, either at the expiry of the Initial Term or as otherwise provided in this Agreement, will not constitute an expropriation by the Province or be tantamount to an expropriation by the Province at domestic or international law (including, but not limited to the *North American Free Trade Agreement*), and will not constitute grounds for asserting any Claim whatsoever under any domestic law, international agreement, or domestic law implementing an international agreement (including, but not limited to, Chapter Eleven of the *North American Free Trade Agreement* and the *General Agreement on Trade in Services*).

2.5 Renewal Option.

The Province, at its sole option and acting in its discretion, may elect to renew:

(a) the Initial Term DC Services for one (1) additional renewal term of five (5) years expiring on March 31, 2029 (the "**Renewal Term DC Services**"); and

(b) the Initial Term Managed Services for two (2) additional renewal terms, the first such renewal term being for three (3) years expiring on March 31, 2024 and the second such renewal term being for five (5) years expiring on March 31, 2029 (collectively the "**Renewal Term(s) Managed Services**").

The Province may elect to renew either or both of the Initial Term DC Services and the Initial Term Managed Services, and may elect to renew any Renewal Term(s) Managed Services, as the case may be, by delivering written notice of such renewal to the Service Provider in accordance with the provisions of Section 2.6 (*Renewal Notice*), but subject to the provisions of Section 2.7 (*Renewal Negotiations*). No such renewal of the Initial Term DC Services, the Initial Term Managed Services, or any Renewal Term(s) Managed Services, as the case may, be will prevent either Party from exercising its rights to terminate this Agreement in accordance with its terms. If the Province elects to renew the Initial Term DC Services or the second and final Renewal Term Managed Services such that the term for such services extends past the Initial Term of this Agreement, then the Initial Term of this Agreement shall automatically be renewed for a period of five (5) years expiring on March 31, 2029.

For greater clarity, the table below sets forth the renewal terms for the Agreement, the Data Centre Services and the Managed Services.

	Initial Term	**Renewal Term**	**Renewal Term**
Agreement	15 years	_____	5 years
DC Services	15 years	_____	5 years

Managed Services	12 years	3 years	5 years

* If the Province elects to renew the Initial Term DC Services or the second and final Renewal Term Managed Services then the Initial Term of the Agreement shall be automatically be renewed.

2.6 Renewal Notice.

Where the Province intends to renew the Initial Term DC Services or the Initial Term Managed Services or a Renewal Term(s) Managed Services, as the case may be, the Province will provide the Service Provider with eighteen months prior written notice of such intention. If the Province does not deliver such notice to the Service Provider on or before such date, then the Province will be deemed to have elected not to renew the Initial Term DC Services or the Initial Term Managed Services or a Renewal Term(s) Managed Services, as the case may be.

2.7 Renewal Negotiations.

The terms and conditions of this Agreement will apply during the Renewal Term DC Services or any Renewal Term(s) Managed Services except for the following, which will be subject to renegotiation and agreement by the Parties acting in good faith (which renegotiations will commence following receipt of a renewal notice by the Service Provider):

(a) in the case of a complete renewal of all of the Data Centre Services or Managed Services, as applicable (which renewal will only be effective if the Parties are able to agree upon all of the terms thereof within the time required pursuant to this Section):

(i) the provisions of Section 15.3 (*Method of Payment*), Schedule 11 (*Service Levels*), Section 12 (*Service Level Failures*), **Schedule 18** (*Governance*) and **Schedule 23** (*Fees*), and

(ii) such provisions of this Agreement which may require consequential amendments as a result of the foregoing; or

(b) in the case of a partial renewal of some but not all of the Data Centre Services or Managed Services, as applicable (which partial renewal will only be effective if the Parties are able to agree upon all of the terms thereof within the time required pursuant to this Section):

(i) the part of the Data Centre Services or Managed Services, as applicable under this Agreement to be performed by the Service Provider during the Renewal Term DC Services or any Renewal Term(s) Managed Services, as the case may be (and for greater clarification, the determination and negotiation thereof will be for purposes of identifying such partial Data Centre Services or Managed Services, and not for purposes of creating new partial Data Centre Services or Managed Services that are not otherwise included in the Data Centre Services or Managed Services then performed by the Service Provider prior to the applicable Renewal Term DC Services or any Renewal Term(s) Managed Services),

(ii) the provisions of **Schedule 6** (*Basic Services*), Schedule 11 (*Service Levels*), Section 12 (*Service Level Failures*), **Schedule 18** (*Governance*) and **Schedule 23** (*Fees*) as they relate to the partial Renewal Term DC Services or any Renewal Term(s) Managed Services to be performed during the Renewal Term, and

(iii) such provisions of this Agreement which may require consequential amendments as a result of the foregoing.

If the Parties are able to successfully conclude an agreement within the foregoing six (6) months permitted for the renewal discussions, then they will execute a renewal agreement (the "**Renewal Agreement**") on or before the expiry of such period setting forth the negotiated terms that will apply to the Renewal Term DC Services or any Renewal Term(s) Managed Services, as the case may be, which terms will be effective from and after April 1, 2024, being the first calendar day following the expiry of the applicable Initial Term DC Services, Initial Term Managed Services or Renewal Term(s) Managed Services (as such date may be extended pursuant to Section 2.8 (*One Year Extension*)), or such other date as may be agreed to in writing by the Parties. If the Parties fail to agree upon the foregoing terms and fail to execute the Renewal Agreement on or before April 1, 2024, or such other date as may be agreed to in writing by the Parties, then there will be deemed to be no Renewal Term DC Services or Renewal Term(s) Managed Services (or subsequent Renewal Term(s) Managed Services), as the case may be, for this Agreement (whether for a partial renewal or a full renewal of the Data Centre Services or the Managed Services, as applicable), and subject to Section 2.8 (*One Year Extension*), the Initial Term DC Services or the Initial Term Managed Services, or to the extent applicable and Renewal term Managed Services, will expire at the end of thereof or earlier in accordance with the terms of this Agreement.

2.8 One Year Extension.

The Province, at its sole option and acting in its discretion, may elect to extend either or both of the Data Centre Services or the Managed Services each for one (1) additional twelve (12) month period (each, an "**Extension**"), by delivering written notice of such extension to the Service Provider in accordance with the provisions of Section 2.9 (*Extension Notice*), but subject to the following:

(a) the Province will only be entitled to one Extension in respect of the Data Centre Services which will only apply to the last applicable "term" of the Data Centre Services, being either the Initial Term DC Services or the Renewal Term DC Services, as the case may be;

(b) the Province will only be entitled to one Extension in respect of the Managed Services which will only apply to the last applicable "term" of the Managed Services, being one of the Initial Term Managed Services or the last applicable Renewal Term(s) Managed Services, as the case may be, and provided that:

(i) the Province will only be entitled to an Extension in respect of the end of the first Renewal Term Managed Services if, in connection with such Extension, either: (A) the Province also elects to extend the Initial Term Data Centre Services for the one (1) additional twelve (12) month period; or (B) the Province and the Service Provider enter into an agreement for the renewal of the Data Centre Services for the Renewal DC Services Term; and

(ii) the Province will only be entitled to an Extension in respect of the end of the second Renewal Term Managed Services if, in connection with such Extension, either: (A) the Province also elects to extend the Initial Term Data Centre Services for the one (1) additional twelve (12) month period; or (B) the Province ensures the Person performing data centre services to the Province during the second Renewal Term Managed Services continues to provide, during the Extension, substantially the same data centre services as were being provided and on the substantially the same terms and conditions as were in effect prior to the Extension, and

(c) if the Province elects to extend the Data Centre Services or the Managed Services as contemplated in the provisions above such that the term for such services extends past the term of this Agreement, then this Agreement shall automatically be extended to a corresponding date.

The Parties acknowledge that the purpose for granting the Province the Extension of the Data Centre Services and the Managed Services is to allow the Province to conclude any procurement or other related process that it may undertake in connection with the selection of a new service provider for the Data Centre Services and/or the Managed Services or the repatriation of all or part thereof in-house with the Province, as the case may be.

2.9 Extension Notice.

Where the Province intends to extend the Data Centre Services or the Managed Services as contemplated under Section 2.8 (*One Year Extension*) above, as the case may be, it will provide the Service Provider with prior written notice of its election to extend as follows:

(a) in the case of the Data Centre Services, on or before the following dates, as applicable:

(i) if the Extension applies to the Initial Term DC Services, then on or before March 31, 2023; or

(ii) if the Extension applies to the Renewal Term DC Services, then on or before March 31, 2028; and

(b) in the case of the Managed Services, on or before the following dates, as applicable:

(i) if the Extension applies to the Initial Term Managed Services, then on or before March 31, 2020; or

(ii) if the Extension applies to a Renewal Term(s) Managed Services, then on or before twelve (12) months before the expiry of the applicable Renewal Term(s) Managed Services.

If the Province does not deliver such notice to the Service Provider within the time required, then the Province will be deemed to have elected not to have an Extension of the Data Centre Services and/or the Managed Services, as the case may be.

2.10 Extension Terms.

Unless otherwise agreed to in writing by the Parties, the terms and conditions in effect as at the end of the Initial Term DC Services, the Renewal Term DC Services, the Initial Term Managed Services or any applicable Renewal Term(s) Managed Services, as the case may be, being the terms and conditions set forth in this Agreement as amended, changed, modified or supplemented by the Parties in the manner contemplated under this Agreement, will apply during an Extension of the Data Centre Services or the Managed Services, as applicable.

2.11 Termination Assistance.

In connection with the expiry of any (and each) Initial Term DC Services, the Renewal Term DC Services, the Initial Term Managed Services or applicable Renewal Term(s) Managed Services (as the same may be renewed or extended as contemplated under this Agreement), or earlier termination thereof,

the Service Provider will provide the Termination Services to the Province in accordance with Article 29 (*Termination Services*).

2.12 Effect of Termination.

The expiry or earlier termination of this Agreement will cause, and will be deemed to cause, the expiry or earlier termination of all other Transaction Documents as of the same date, except for those provisions in this Agreement and in the other Transaction Documents, which are stated to survive Termination.

ARTICLE 3 – INITIAL TRANSITION

3.1 Master Transfer Agreement/Transition Plan.

Each Party will perform its respective obligations as set out in the Master Transfer Agreement and in the Transition Plan, in accordance with their respective terms.

3.2 Hand-Over of Services.

Subject to the provisions of this Article 3 (*Initial Transition*), the Parties will transfer responsibility and accountability for the provision of the Services to the Service Provider (the "**Transition**"), with effect on the Hand-Over Date. In connection therewith, the Service Provider will commence the delivery of the Services on the Hand-Over Date, other than those Services that are expressed in this Agreement as being Services that are to be commenced by the Service Provider on some date other than the Hand-Over Date (such as the Transition Services and the Termination Services).

3.3 Transition Services.

For purposes of completing the Transition, and from and after the execution of this Agreement, the Service Provider will provide the following services to the Province (collectively, the "**Transition Services**"):

(a) such services as are necessary to complete the Transition by the Hand-Over Date and in a manner that will, to the greatest extent possible, ensure the continued, uninterrupted and efficient delivery of the Services throughout the transition, and that will minimize any disruption to the business operations of the Province;

(b) the complete and timely performance by the Service Provider of all matters required to be performed by or on behalf of the Service Provider, or for which the Service Provider is otherwise responsible, in accordance with the initial transition plan attached to this Agreement as **Schedule 2** *(Transition Plan)*, as such transition plan may be amended, modified and supplemented in accordance with the provisions of Section 3.4 (*Modifications to Transition Plan*) (collectively, the "**Transition Plan**"); and

(c) the Service Provider will be responsible for the overall management and implementation of the Transition, including coordinating, planning and implementing the Transition in accordance with the Transition Plan and this Agreement.

3.4 Modifications to Transition Plan.

Notwithstanding the level of detail contained in the initial Transition Plan, the Parties acknowledge that the initial Transition Plan may require modifications after the execution of this Agreement. Such modifications will be agreed to by the Parties in accordance with the Transition Governance Process, and

once agreed to through the Transition Governance Process, such modifications will be incorporated into the Transition Plan, and the Transition Plan will be deemed to be amended accordingly (including amending **Schedule 2** *(Transition Plan)*). For greater clarification, the Parties confirm that any changes to the following in respect of the Transition Plan will require the joint Approval of the Parties through the Province's STMS AMO Lead and the Service Provider's STMS Lead:

(a) the Hand-Over Date; and

(b) the scope of the Services to be provided by the Service Provider as of the Hand-Over Date.

3.5 Transition Management.

During the Transition Period and for one month after the Hand-Over Date, each Party will assign a transition management team (each a "**Transition Management Team**"), comprised of the members as set forth in **Schedule 3** *(Transition Management and Governance)*, who will be primarily dedicated to the implementation of the Transition. The guiding principles, responsibilities and meeting process for meetings between members of each Transition Management Team will be as set forth in **Schedule 3** *(Transition Management and Governance)*. For greater clarification, **Schedule 3** *(Transition Management and Governance)* includes a governance process to monitor progress and identify any issues or circumstances that may impact the schedule set forth in the Transition Plan (the "**Transition Governance Process**"). Any potential delays or circumstances that may adversely affect the Transition will be escalated in accordance with the Transition Governance Process in lieu of the Change Order Process.

3.6 Completion of Transition Plan.

Subject to Sections 3.9 (*Failure to Complete Transition Plan*) and 3.10 *(Effect of Termination Prior to Hand-Over Date*), the transfer of the provision and performance of the Services to the Service Provider will be subject to the completion of the requirements of the Transition Plan before the Hand-Over Date. Such requirements of the Transition Plan will be completed at such time as:

(a) all components of the Transition Plan that are required under the terms of the Transition Plan to be completed prior to the Hand-Over Date have been completed; or

(b) the Service Provider and the Province, through the Transition Governance Process, have jointly waived the requirement to complete any such component of the Transition Plan that has not been completed prior to the Hand-Over Date, or have transferred the obligation of the Service Provider (or other applicable Person) to complete the same after the Hand-Over Date.

The Service Provider will complete all components of the Transition Plan (if any) that are required under the terms of the Transition Plan to be completed after the Hand-Over Date, within the times indicated in the Transition Plan.

3.7 Transition Costs.

Other than the payment of the applicable Fees expressly set forth in Article 15 (*Fees and Payment Terms*) which are the responsibility of the Province, the Service Provider is responsible for all of the costs incurred by the Service Provider (or its Subcontractors) for completing the Transition Plan, including all direct and indirect costs incurred by the Service Provider (or its Subcontractors) in connection with the

implementation of the Transition Plan, and the overall management of the Transition Plan, but excluding therefrom:

(a) those costs, if any, identified in the Master Transfer Agreement as being the responsibility of the Province; and

(b) those costs incurred by the Province in connection with the Transition Plan.

3.8 Work-in-Progress Projects.

The Parties acknowledge that there are certain Work-in-Progress Projects existing as of the date of this Agreement in respect of which there may be work that will not be completed by the Hand-Over Date, and that will constitute work-in-progress as of such date, as more particularly described in **Schedule 4** *(Work-in-Progress Projects)*. The Parties will handle the Work-in-Progress Projects in accordance with the following principles:

(a) the Province will have financial and operational responsibility for the Work-in-Progress Projects prior to the Hand-Over Date; and

(b) from and after the Hand-Over Date, the Service Provider will assume operational responsibility for the Work-in-Progress Projects that have not been completed by the Hand-Over Date, which will be paid for in accordance with the provisions of **Schedule 23** *(Fees)*.

3.9 Failure to Complete Transition Plan.

If the Transition Plan is not completed, as applicable, by the Hand-Over Date and the Parties are unable to agree upon which Party caused the delay, then the matter of fault for purposes of determining whether the delay was caused by one Party or the other, will be deemed to be a Dispute and will be determined in accordance with the Dispute Resolution Process under Article 27 (*Dispute Resolution*). For greater clarification, no Party will be deemed to have failed to perform its obligations under the Transition Plan where such performance is dependent upon the performance by the other Party of that other Party's obligations under the Transition Plan, in circumstances where that other Party has failed to so perform.

3.10 Effect of Termination Prior to Hand-Over Date.

If this Agreement is terminated prior to the Hand-Over Date, then the following provisions will apply:

(a) the obligations of the Parties to continue to pursue the transactions and the contractual relationship contemplated in this Agreement and in the other Transaction Documents will immediately terminate and cease to be of any further force or effect;

(b) this Agreement will terminate and cease to be of further force or effect subject to survival of those provisions specified in Section 33.11 (*Survival*) of this Agreement;

(c) each of the other Transaction Documents, if executed and delivered, will terminate and cease to be of any further force or effect subject to survival of any provisions contemplated therein or herein to survive termination of the applicable Transaction Documents, and any assets transferred in respect of such Transaction Documents prior to such date will be transferred back to the original Party on the same terms as initially transferred;

(d) the Service Provider will, forthwith after the Termination Date or the expiry of the Termination Assistance Period, which ever is the later, return to the Province (or at the direction of the Province destroy) all of the Province Confidential Information and Province Records provided to the Service Provider prior to the Termination Date (including prior to the execution of this Agreement pursuant to the JSD Agreement), and will not retain and will destroy all copies thereof which the Service Provider (or any Subcontractor, agent, consultant or Person working for or hired by or on behalf of the Service Provider in connection with this Agreement, the Transaction Documents and the transactions contemplated herein and therein) may have made or caused to be made;

(e) where this Agreement is terminated as a result of a failure to complete the Transition by the Hand-Over Date for any reason other than the fault or delay of the Province, then the Service Provider will not be entitled to receive any payment or compensation from the Province; and

(f) where this Agreement is terminated by the Province as a result of a failure to complete the Transition by the Hand-Over Date due solely to the fault or delay of the Province, then the Service Provider will not be entitled to receive any payments or other compensation from the Province except as expressly provided for in **Schedule 38** *(Termination Fees)* in respect of a Termination effected pursuant to this Section 3.10 (*Effect of Termination Prior to Hand-Over Date*).

ARTICLE 4 – SERVICES

4.1 Overview of Services.

Subject to a Partial Commencement of the Services pursuant to Article 3 (*Initial Transition*), as may otherwise be agreed to by the Parties in accordance with the Change Order Process, and as may be transformed and otherwise changed in accordance with the provisions of this Agreement during the Term, the Service Provider will provide to the Province, and the Province will obtain from the Service Provider, the following services from and after the Hand-Over Date (or from and after such other date as indicated below), upon the terms and conditions set forth in this Agreement (collectively, the "**Services**"):

(a) the Transition Services, as more particularly described in Article 3 (*Initial Transition*), from and after the Effective Date;

(b) the basic services described as such in **Schedule 6** *(Basic Services)* (which includes the inherent services described in Section 4.2 (*Included or Inherent Services*), as such Schedule may be amended and supplemented by the Parties from time to time in accordance with this Agreement (collectively, the "**Basic Services**");

(c) the transformed services in accordance with Article 6 (*Transformation*), being the Basic Services as described in **Schedule 6** *(Basic Services)* as transformed pursuant to the Transformation Plan (collectively, the "**Transformed Services**");

(d) the Termination Services, as more particularly described, and within the times indicated, in Article 29 (*Termination Services*);

(e) such other services or additional services as may be agreed to by the Parties pursuant to the Change Order Process; and

(f) all such other or additional services as set forth or otherwise described in this Agreement.

4.2 Included or Inherent Services.

The Parties acknowledge that there are functions or tasks not specifically listed or described in this Agreement that are customarily required for the proper performance and provision of the Services (as the same may be improved, changed or transformed as contemplated under this Agreement), or as may otherwise be required to perform the Services in a manner consistent with the performance thereof prior to the Hand-Over Date. Without limiting the foregoing and subject to the provisions of this Section, such functions or tasks will be deemed to be implied or included in the scope of the Services to the same extent and in the same manner as if those functions or tasks had been specifically described in this Agreement. Notwithstanding the foregoing, this Section is not intended to expand the scope of the Services beyond the Services described in this Agreement, or to require a higher standard of Service delivery than that which is otherwise described in this Agreement.

4.3 Language of Services.

The Service Provider will provide all of the Services in English, and in such other languages and with such other special arrangements to accommodate Clients and Stakeholders with visual, hearing and other similar forms of special needs, as set forth in **Schedule 7** *(Language of Services)*.

4.4 Standard of Care.

Unless specifically provided otherwise in this Agreement (or in any schedules attached to this Agreement), the Service Provider will provide the Services under this Agreement using the standard of care of a reasonable service provider performing similar services in comparable circumstances.

4.5 Services and Program Changes.

All changes, modifications, amendments or supplements to the Services provided by the Service Provider to the Province under this Agreement will be undertaken in accordance with the Change Order Process and any other express provisions of this Agreement that contemplate changes to the Services.

4.6 Service Recommendations.

As part of the Services, the Service Provider will, from time to time as it may deem appropriate, but not less frequently than annually, make recommendations to the Province for improvements to the Services based on changes and trends in the data centre services and server hosting and mainframe services field and available new technologies, and implement any of such recommendations Approved by the Province in accordance with the Change Order Process.

4.7 Quality Management.

In providing the Services to the Province during the Term, the Service Provider will:

(a) be responsible for implementing and carrying out continuous improvement and quality management for all of the Services;

(b) establish quality assurance programs that encompass continuous improvement of the Services in addition to an ongoing quality assessment of the Services;

(c) maintain an ongoing focus on the satisfaction of the Province, the Clients and the Stakeholders, as well as other users of the Services, by monitoring and evaluating trends

that develop in the performance of the Services (as indicated through complaint processes or otherwise), and by making recommendations to the Province in respect thereof; and

such activities will be performed entirely by the Service Provider at its own expense and will not require the resources of the Province or the payment of any additional Fees without the Approval of the Province.

4.8 Documentation.

The Service Provider will deliver to the Province a detailed and comprehensive operational procedures manual in respect of the Services (the "**Manual**"), in a form and substance that is subject to the Province's prior consultation, and containing the matters referred to in Section 4.9 (*Manual Requirements*), within six (6) months after the Hand-Over Date. The Service Provider will periodically, but not less than quarterly unless otherwise agreed by the Province, update the Manual to reflect changes in the operations or procedures described in the Manual. The Service Provider will provide the Province with the updates of the Manual on a timely basis, and within the period required for such updates to be made, for consultation with the Province. For greater clarification, the Parties acknowledge that the Manual is intended to describe to the Province how the Services will be performed, and will in no event be interpreted so as to relieve the Service Provider of any of its performance obligations under this Agreement. The consultation with the Province under this Section 4.8 (*Documentation*) is not intended to, and will not be deemed to, shift the risk and responsibility for the business operations in performing the Services from the Service Provider to the Province, and the Parties acknowledge and agree that the responsibility and risk thereof will remain at all times with the Service Provider.

4.9 Manual Requirements.

The Manual will describe or include the following:

(a) the procedures associated with the business processes and technology support services that the Service Provider will undertake in order to provide the Services;

(b) the methods of operation and procedures the Service Provider will use to perform the Services, such as network topologies, security administration, system configurations, call centre processes, human resource functions, business processes and associated documentation that provides further details of such activities, as applicable (including, for example, user support manuals, job scheduling procedures, specifications and updates of such materials); and

(c) current documentation with respect to the Systems, business processes, and processes in support of the operations and procedures used to deliver the Services (which documentation will be sufficient to enable the Province, or another service provider that is reasonably skilled in the provision of services similar to the Services, to fully assume the provision of the Services), and the Manual will detail how such documentation will be maintained.

4.10 Knowledge Transfer.

The Service Provider acknowledges that the Province needs to retain an appropriate level of understanding regarding the manner in which the Services are delivered throughout the Term. As part of the Basic Services, the Service Provider will provide the Province with ongoing knowledge transfer with respect to the Services in the manner Approved through the Governance Process or as otherwise requested by the Province from time to time. The Service Provider will provide such knowledge transfer to the Province at the level of information and detail as may be required by the Province to ensure that the

Province is a well informed customer regarding the manner in which the Services are delivered. At the request of the Province, the Service Provider will provide any new Province staff (who have duties related to the Services or the Service Provider) with an orientation and training regarding the manner in which the Services (or such portion of the Services as may be applicable under the circumstances) are delivered by the Service Provider, and at such mutually scheduled times as may be reasonably agreed to by the Parties through the Governance Process. The Service Provider will also provide the Province and its staff with information and general training sessions regarding any significant process or Systems changes that may occur in respect of the Services throughout the Term.

4.11 Province Retained Responsibilities.

During the Term (and without limiting any other provisions of this Agreement regarding the responsibilities of the Province), the Province will remain responsible for and will retain control of the following:

(a) setting all Province Policies and guidelines including, without limitation, those relating to the Services, records management, and privacy and security;

(b) all media relations, including the Approval of the Service Provider media communications, Client communication and Stakeholder communications in accordance with Article 10 (*Branding and Communications*);

(c) the exercise of powers for and on behalf of Her Majesty the Queen in Right of the Province of British Columbia, as represented by the Minister of Labour and Citizens' Services;

(d) any all relations with Clients and Stakeholders; and

(e) such other direct responsibilities as may be expressly contemplated in this Agreement.

The Parties acknowledge that these responsibilities are vested solely in the Province. The Service Provider has no right or obligation to exercise any responsibilities of the Province set forth in this Section and is not accountable for actions taken by the Province in respect of the same. For greater clarification, where the Province exercises its responsibilities under this Section 4.11 (*Province Retained Responsibilities*) and such exercise affects the Service Provider in the manner contemplated in the Change Order Process, then the provisions of Article 7 (*Change Order Process*) will apply, as applicable.

4.12 Failure of Province to Perform Retained Responsibilities.

In the event of (i) a failure by the Province to perform its obligations under this Agreement (other than a failure to make payments in accordance with Section 28.3 (*Material Breach by Province*), (ii) a failure by the Province to provide services to the Service Provider as specifically provided in this Agreement, if any, to the extent that the Services are contingent upon the performance by the Province thereof, or (iii) the Province Intellectual Property utilized or otherwise accessed by the Service Provider under license or access rights pursuant to Sections 19.8 (*License to Use Province Proprietary Software for the Services*) and 19.9 (*Use of Province Licensed Software*) infringing the Intellectual Property rights of a third party, such that the Service Provider is unable to utilize such Province Intellectual Property, then the following provisions will apply:

(a) the Service Provider will notify Province through the Hosting Alliance Management Office Lead, as soon as possible, and in any event within five (5) Business Days from the date the Service Provider discovers that such failure or infringement has occurred,

providing details with respect to such failure or infringement (such as the specific obligation or co-operation sought, the individuals from whom it was sought, and the date such request was made);

(b) the Service Provider and the Province, through the Governance Process, will promptly meet in order to discuss and resolve, if possible, the failure or the infringement;

(c) unless the Province contests the Service Provider's assertion that such failure or infringement has occurred, the Province will address such failure, make reasonable efforts to either negotiate a license or access rights in respect of the Province Intellectual Property in question, provide a "workaround" to address the failure or infringement, or provide alternative Intellectual Property as a replacement for the infringing Province Intellectual Property, all as applicable under the circumstances;

(d) if such failure of the Province or infringement has a material impact on the delivery and performance of the Services or on the cost of providing the Services, then effective as of the date that the notice of the failure or infringement is delivered to the Province in accordance with paragraph (a) above, the Service Provider and the Province will adjust the Fees, time frames for performance, Service Levels or Services, as applicable and to the extent affected, either on a temporary basis or a long term basis, in accordance with the Change Order Process;

(e) if the Service Provider does not so notify the Province of the failure or infringement as set forth in this Section, then such failure or infringement on the part of the Province will not excuse, or be used as a defence for, the Service Provider's failure to perform its obligations under this Agreement;

(f) for greater clarification, the Parties acknowledge that the Service Provider has the right to elect not to immediately deliver notice to the Province under paragraph (a) above for minor failures, with such election in no way restricting the Service Provider from subsequently delivering a notice under paragraph (a) above that is in respect of all such minor failures (to the extent that they continue to impact delivery of the Services), all of such failures thereafter being deemed, for the purposes of this Section, to be a single failure by the Province to perform in accordance with its obligations under this Agreement;

(g) any failure of the Province Shared Infrastructure will not be governed by this Section but will instead be governed by the provisions set forth in Article 20 (*Province Shared Infrastructure*); and

(h) except as specifically provided otherwise in this Agreement, the application of the foregoing provisions will constitute the sole remedy of the Service Provider in respect of such failure or infringement by the Province.

4.13 Restrictions on Shared Environment.

Unless expressly provided elsewhere in this Agreement or upon the Approval of the Province, the Service Provider will ensure that all Systems and premises that are used to provide the Services are not in any manner shared or otherwise utilized to provide services to any other Person unless expressly Approved by the Province. With respect to any shared Systems or premises that are Approved by the Province, the Service Provider will ensure that all such Systems and premises are segregated and not accessible at any time by any Persons other than those expressly authorized by or in accordance with this Agreement, and

that such Systems and premises are not used for any purposes except for those expressly Approved by the Province. Without limiting the generality of the foregoing, the Service Provider will at all times comply with the privacy, confidentiality and security obligations as set forth in **Schedule 24** *(Privacy Obligations)* and as otherwise set forth in this Agreement. At no time and under no circumstances will any Personal Information or Province Confidential Information be shared or otherwise accessible by any shared System other than the Province Shared Infrastructure (to the extent applicable).

ARTICLE 5 – SERVICE AND DATA LOCATIONS

5.1 Overview of Service Locations.

No Services will be provided or performed by the Service Provider at any location other than the Service Locations, which Services Locations are within Canada, unless permitted under or pursuant to this Agreement. No Personal Information will be accessed, used, stored, transmitted or otherwise made available in any manner outside of Canada, and no Person outside of Canada will have access in any manner to the Personal Information, except as may be specifically permitted under the *Freedom of Information and Protection of Privacy Act* (British Columbia) and Approved in writing by the Province from time to time.

5.2 Service Locations.

The addresses at which any Personal Information will be accessed, used, stored, transmitted or otherwise made available by the Service Provider or its Subcontractors, or from where any Services will be performed (collectively, the "**Service Locations**"), are set forth in the attached **Schedule 8** *(Service Locations)*. The Service Provider will not store any Personal Information databases except in those locations set forth in **Schedule 8** *(Service Locations)* without the Province's Approval, and the Service Provider will ensure that its Subcontractors do not access, use, store, transmit or otherwise make available any Personal Information at any other locations unless the Service Provider provides the Province with prior written notice thereof, and provided that such locations are within British Columbia (or elsewhere in Canada as may be permitted under or pursuant to this Agreement). For greater clarification, nothing contained in this Section will permit or otherwise enable the Service Provider (or any of its Subcontractors) to perform the Services from a location outside of British Columbia unless permitted under or pursuant to this Agreement or otherwise Approved by the Province.

5.3 Relocation of the Service Provider Service Locations.

The Service Provider may relocate all or a part of the Services at any time upon prior written notice thereof to the Province, provided that:

(a) the Service Provider will not permit its Personnel or any External Personnel to work from home or engage in other similar remote telecommunicating activities, where the same involve the use of Personal Information, without the prior Approval of the Province through the Change Order Process; and

(b) the relocation of all or any portions of the Services will be subject to the Approval of the Province, which will not be unreasonably withheld (acknowledging that the Province will grant or withhold such Approval having regard to the interests of the Province, the Clients and the Stakeholders).

5.4 Service Location Policies.

To the extent applicable, at all times while accessing any premises of the other Party (including the premises of any applicable subcontractors of that other Party) in connection with the Services being performed under this Agreement, or as may otherwise be contemplated under this Agreement, each Party will, and will cause their respective personnel, external personnel, subcontractors, representatives or other parties for whom they are responsible at law or under the terms of this Agreement to, comply with any standard workplace security, safety, operational and other similar policies and procedures applicable to visitors for such Party, as may be notified by each Party to the other from time to time. The foregoing will not in any way limit or otherwise prohibit the Province from exercising its rights under Article 22 (*Audit Rights*).

ARTICLE 6 – TRANSFORMATION

6.1 Transformation Program.

Each party will be responsible for their respective obligations in connection with the Transformation Projects, in accordance with the provisions set forth in **Schedule 9** *(Transformation)*.

6.2 Transformation Plan.

The Transformation Projects will be conducted in accordance with the transformation plan prepared by the Service Provider, including the completion dates set forth in the transformation plan, an initial copy of which is attached as **Schedule 10** *(Transformation Plan)*, and as such initial transformation plan may be amended, modified and supplemented as contemplated in Section 6.3 *(Modifications to Transformation Plan)* (collectively, the "**Transformation Plan**"). Any such modifications to the Transformation Plan, once agreed to by the Parties in accordance with Section 6.3 *(Modifications to Transformation Plan)*, will be incorporated into the Transformation Plan, and the Transformation Plan will be deemed to be amended accordingly (including amending **Schedule 10** *(Transformation Plan)*).

6.3 Modifications to Transformation Plan.

Notwithstanding the level of detail contained in the initial Transformation Plan attached as **Schedule 10** *(Transformation Plan)*, the Parties acknowledge that the initial Transformation Plan may require modifications after the execution of this Agreement. Such modifications will be agreed to by the Parties in accordance with the Change Order Process, and once agreed to through the Change Order Process, any such modifications will be incorporated into the Transformation Plan, and the Transformation Plan will be deemed to be amended accordingly. In connection with any such modifications to the Transformation Plan, the Service Provider will ensure that the Transformation Plan, as so modified, adequately addresses the following:

(a) policy compliance and operational impact;

(b) standards adherence and privacy and security;

(c) a detailed description of each stage and applicable completion dates for each stage Transformation Projects; and

(d) such other matters as may be applicable in the circumstances.

6.4 Disputes Regarding the Transformation Plan.

If modifications are required to be made to the Transformation Plan as contemplated under Section 6.3 (*Modification to Transformation Plan*), and the Parties are unable to agree upon all or any matter relating to such modifications to the Transformation Plan in accordance with the Change Order Process, then the matter will be deemed to be a Dispute and will be settled between the Parties in accordance with the process described in Section 27.3 (*Expedited Arbitration*).

6.5 Delay in Completion of Transformation.

Each stage of each of the Transformation Projects will have a completion date for the particular stage as set forth in the Transformation Plan. Where the date for any stage is past the applicable completion date for the stage, then the Parties will meet to discuss the status of the Transformation and the likelihood of meeting the next stages of the Transformation Plan, as more particularly described in the Transformation SOW. With respect to Section 5 of the Transformation SOW, in the event the applicable completion date for the stage extends beyond the Data Centre Availability Date, then credits will be granted by the Service Provider to the Province (the "**Transformation Credits**") in accordance with the provisions set forth in **Schedule 9** *(Transformation)*. The Province may deduct or off-set the Transformation Credits against the Fees payable by the Province to the Service Provider under this Agreement.

ARTICLE 7– CHANGE ORDER PROCESS

7.1 Ordinary Course Changes.

The Parties acknowledge and agree that the data centre services and server hosting and mainframe services operations and activities of the Province that are the subject of the delivery of Services pursuant to this Agreement are subject to constant changes in the ordinary course of such operations and activities, which changes do not have a material impact on the following (collectively, the "**Ordinary Course Changes**"):

(a) the delivery and performance of the Services; or

(b) the cost of providing the Services.

The Ordinary Course Changes are within the scope of the Services contemplated under this Agreement and will not result in additional Fees being payable by the Province to the Service Provider. The Ordinary Course Changes may be implemented without the need for a formal Change Order. Notwithstanding the foregoing, the Service Provider will maintain a record of each Ordinary Course Change that occurs in the Services, and will provide the Province, through the Governance Process, with monthly reports detailing the same.

7.2 Province Initiated Ordinary Course Changes.

The Province may require the Service Provider to implement any Ordinary Course Change by written notice to the Service Provider of such change, in which event the following provisions will apply:

(a) no formal documentation requesting the Ordinary Course Change is required and the Province may request the Ordinary Course Change by any form of written notice (including electronic forms of notice) to the Service Provider;

(b) the Approval or agreement of the Service Provider to an Ordinary Course Change requested by the Province is not required, and the Service Provider will implement the

Ordinary Course Change as soon as reasonably practicable following receipt by the Service Provider of a written notice from the Province requesting it to do so; and

(c) the Parties will cause a record of each Ordinary Course Change to be maintained as contemplated in Section 7.1 (*Ordinary Course Changes*).

7.3 Other Changes.

In addition to the Ordinary Course Changes, the Parties acknowledge that certain changes may be required or desirable which exceed or are otherwise outside of the definition of Ordinary Course Changes. Such changes may include, without limitation, the following:

(a) the addition or removal of material Services ;

(b) changes to a Service Level (including the addition or removal of Services Levels);

(c) a material change to the technology or Systems used in the performance of the Services;

(d) a permanent change that has a material impact on the delivery or cost of the Services;

(e) a change that has an material impact on the Privacy Obligations;

(f) a change in the locations from where the Services are primarily performed; and

(g) any other matter that the Parties may agree as properly being the subject of the Change Order Process.

7.4 Change Request.

Either Party may initiate the change process described in Sections 7.4 (*Change Request*) to 7.12 (*Record of Changes*) (collectively, the "**Change Order Process**") in connection with a change described in Section 7.3 (*Other Changes*) by submitting to the other Party, through the Governance Process, a written notice signed by the initiating Party, which notice will include all relevant information reasonably required for the proper consideration of such change or for the commencement of the Change Order Process in respect thereof (each, a "**Change Request**").

7.5 Change Request Process.

Following the delivery of a Change Request by one Party to the other, the following will apply:

(a) the Parties will meet together through the Governance Process to clarify the Change Request and confirm the requirements of the Change Request including, without limitation, details regarding the time requirements to consider the Change Request (it being acknowledged by the Parties that the time required may vary depending upon the nature and complexity of the proposed change);

(b) upon receipt of a Change Request from the Province, the Service Provider will prepare a proposal (the "**Proposal**") within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process, acting reasonably and having regard to the nature and complexity of the Change Request in question), which Proposal will include a privacy assessment of the collection, use, disclosure and retention of Personal Information and a threat and risk assessment (in such form as may be required

by the Province), as well as a description of the impact of the proposed change on the following (to the extent applicable having regard to the nature of the proposed change):

(i) the costs of implementation,

(ii) the rights and obligations of the Parties under this Agreement with respect to, or as a result of, the proposed change,

(iii) the Services,

(iv) the Service Levels,

(v) any technology, Systems or operations of the Service Provider used in the Services, the Province, the Clients, the Stakeholders or any customers of the Services,

(vi) an increase or decrease to the Fees payable under this Agreement,

(vii) the Privacy Obligations, and

(viii) any other relevant matter related to this Agreement that will be materially impacted (both positively and negatively);

(c) if the Service Provider initiates the Change Request, then the Service Provider will prepare and deliver a Proposal to the Province within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process, acting reasonably and having regard to the nature and complexity of the Change Request in question) following the meeting of the Parties to clarify the Change Request, as contemplated in paragraph (a) above;

(d) the Province will provide the Service Provider with a written response to the Proposal within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process) of receipt of the Proposal from the Service Provider, indicating the Province's Approval of the Proposal, its rejection of the Proposal (indicating the reasons therefor), or the terms of a counter proposal acceptable to the Province;

(e) any Proposal Approved by the Province will constitute a Change Order, and will be implemented by the Service Provider in accordance with the particulars of the Change Order;

(f) the Service Provider will be required to respond to all Change Requests received from the Province and to prepare a Proposal in respect thereof;

(g) the Service Provider will not reject a Change Request initiated by the Province unless the Service Provider is unable to make the changes contemplated in the Change Request as a result of technical impediments that are commercially unreasonable to overcome, or the Change Request will result in a material adverse effect on the Service Provider's ability to meet Service Levels, comply with the Privacy Obligations or comply with other material terms or conditions of this Agreement (each an "**Adverse Impact**"). The Service Provider will provide the Province with a written explanation of any Adverse Impact stating in detail the particulars of the Adverse Impact and suggesting reasonable

alternatives or workarounds (to the extent possible) for consideration by the Province in respect thereof; and

(h) if the Province requires that the Change Request be implemented as requested, notwithstanding the Adverse Impact to the Service Provider, then the impact of the Change Request on the Fees, the Service Levels, the Privacy Obligations or other material terms and conditions of this Agreement will be addressed through the Governance Process. If a mutually acceptable resolution is not reached in respect of the proposed Change Request, then the matter will be treated as a Dispute to be resolved pursuant to the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*).

7.6 Change Request Impact on Fees.

If a Change Request has an impact on the Fees that may result in either an increase or decrease to the Fees, then the Parties will determine any increase or decrease to be made to the Fees as a result of such impact in a manner that is consistent with the determination of the amounts as set forth in **Schedule 23** (*Fees*).

7.7 Mandatory Changes.

The Province may require the Service Provider to implement a Change Request before it has become a Change Order (each a "**Mandatory Change**") in situations where:

(a) the Parties are unable to agree upon the Change Request and associated Proposal for any reason;

(b) due to time constraints, the Parties are unable to use, fully complete or otherwise commence the processes set forth in Sections 7.4 (*Change Request*) to Section 7.6 (*Change Request Impact on Fees*); or

(c) due to the urgency of the circumstances surrounding the need for the Mandatory Change, the Province requires that the Service Provider implement the changes forthwith.

The Mandatory Changes will be implemented by the Parties in accordance with the provisions of Section 7.8 *(Implementation of Mandatory Changes)*.

7.8 Implementation of Mandatory Changes.

The Province may require the Service Provider to implement a Mandatory Change by the delivery of a written request (each, a "**Mandatory Change Request**") to the Service Provider, in which case the following provisions will apply:

(a) the Mandatory Change Request will comply with the requirements of Section 7.4 *(Change Request)*;

(b) the Approval or agreement of the Service Provider to the Mandatory Change Request is not required;

(c) the Mandatory Change Request will immediately become a Change Order for the purposes of Section 7.9 *(Change Orders)* upon the issuance by the Province, and the Service Provider will implement the Mandatory Change following receipt of the Mandatory Change Request from the Province, as soon as reasonably practicable to do so;

(d) if, as a result of the Mandatory Change, the Fees are to be increased, decreased or otherwise changed, or any Service Levels, time frames, Privacy Obligations or Services will be impacted, and a determination must be made regarding the particulars of such increase, decrease, change or impact, then the following procedures will apply:

(i) forthwith after receipt from the Province of a Mandatory Change Request in respect of a Mandatory Change, the Service Provider will provide the Province with its proposed adjustment to the Fees and any impact on Service Levels, time frames, Privacy Obligations and Services, in all cases with supporting documentation including, without limitation, detailed information, analysis and back-up support regarding any increase or decrease to the Fees (the "**Impact Assessment**"),

(ii) after the Province has received and reviewed the Impact Assessment from the Service Provider, the Province will, acting reasonably, and after due consideration of the proposed Impact Assessment, and by separate written notice to the Service Provider, set the adjustment to the Fee or such other adjustment or change to the Service Levels, time frames, Privacy Obligations and Services, which adjustment or change will take effect immediately with retroactive effect to the date of the implementation of the Mandatory Change, to the extent applicable under the circumstances,

(iii) if the Service Provider has a Dispute with respect to such adjustment or change, then the Dispute will be settled pursuant to the Dispute Resolution Process set forth in Section 27.3 (*Expedited Arbitration),* and

(iv) the adjustment or change determined by the Province will apply until any Dispute in respect thereof has been resolved between the Parties, whereupon the Parties will make such adjustments as between themselves as may be necessary to give effect to the resolution of the Dispute, retroactive (to the extent possible) to the date of the implementation of the Mandatory Change giving rise to such Dispute;

(e) the costs of implementing a Mandatory Change will be borne by the Service Provider, unless otherwise determined by the Province, acting reasonably, as indicated in its Mandatory Change Request issued with respect to the Mandatory Change or as may otherwise be agreed to by the Parties in writing or determined in the settlement of a Dispute in accordance with paragraph (d)(iii) above; and

(f) the Parties will cause a record of each Mandatory Change and Mandatory Change Request to be maintained as contemplated in Section 7.12 (*Record of Changes*).

7.9 Change Orders.

A Change Request or a Mandatory Change Request will become a "**Change Order**" when the requirements of the procedures to consider such Change Request or Mandatory Change Request set out in this Article 7 (*Change Order Process*) have been satisfied, and the Change Request or Mandatory Change Request is Approved by each of the Parties, where such Approval is required pursuant to this Article 7 (*Change Order Process*).

7.10 Implementation of Change Orders.

The Service Provider will minimize disruption to the delivery of the Services and to the business operations of the Province, the Clients and the Stakeholders as the result of the implementation of a Change Order arising from a Change Request or a Mandatory Change Request. The cost of implementing a Change Order will be borne as set out in the Change Order or as otherwise provided in this Agreement. All privacy reviews contemplated in **Schedule 24** *(Privacy Obligations)* will be conducted in respect of any Change Order as more specifically set forth in **Schedule 24** *(Privacy Obligations)*.

7.11 Consequential Amendments.

If the Parties proceed with a Change Order (whether as the result of a Change Request or a Mandatory Change Request), then the Change Order will constitute an amendment to this Agreement including the relevant Schedules to this Agreement. From and after the effective date of the implementation of a Change Order, this Agreement will be interpreted as amended by the Change Order, and this Agreement, as so amended, will continue in full force and effect for the remainder of the Term.

7.12 Record of Changes.

The Parties will jointly maintain an accurate and complete record of all changes to the Services contemplated in this Article 7 (*Change Order Process*) including all Ordinary Course Changes, Change Requests, Mandatory Change Requests, Mandatory Changes and Change Orders. Such record may be maintained in such form as the Parties may agree pursuant to the Governance Process, including by way of a server-based record accessible by both Parties. Each Party will cooperate to make corrections to such records as the other Party may reasonably request to ensure that the record of all changes is accurate and complete, in all material respects, at all times throughout the Term.

ARTICLE 8 – SERVICE LEVELS

8.1 Overview of Service Levels.

Subject to the specific and more detailed provisions of this Article 8 (*Service Levels*), and any higher standard or level of performance otherwise required in this Agreement which may be applicable in the circumstances, the Service Provider will perform the Services throughout the Term to a standard and level of performance which:

(a) is equal to, or greater than, the standard and level of performance for such Services immediately before the Hand-Over Date; and

(b) will maintain or increase the satisfaction of the Clients of the Services, the Province and Stakeholders.

For greater clarification, the provisions of this Section will apply to all of the Services, including those portions of the Services that are not specifically measured or otherwise monitored through the use of Service Levels.

8.2 General Compliance.

The Parties acknowledge and agree that:

(a) the Service Provider will perform the Services throughout the Term to a standard and level of performance which is required in order for the Service Provider to meet or exceed the Service Levels;

(b) the Service Levels set out in this Agreement, as may be amended from time to time in accordance with this Agreement, are intended to be baseline performance standards and levels for the delivery and performance of the Services;

(c) during the Term, the Service Provider will identify ways to improve or increase the Achieved Service Levels including, without limitation, continually monitoring and evaluating changes and trends in the data hosting and data centre facility services field of operations and monitoring and evaluating new and available technologies and service delivery processes and strategies that are applicable to the Services;

(d) during the Term, the Service Provider will use commercially reasonable efforts to continually improve the quality of the Services and the Achieved Service Levels in a manner consistent with the terms and intent of this Agreement, taking into account the cost of such improvement as compared to the benefit to be derived therefrom; and

(e) any improvements in the Achieved Service Levels or performance standards and levels achieved by the Service Provider in providing the Services, whether or not as part of any progressive improvement requirements contemplated in this Agreement, will not result in an increase in the Fees payable under this Agreement unless otherwise Approved by the Province.

8.3 Transformed Service Levels.

With respect to any Service Levels for the Transformed Services, such Service Levels will only apply after the Acceptance Date for the Stage applicable to such Transformed Services.

8.4 Restrictions on Changes to Service Levels.

The Service Provider acknowledges that the establishment of Service Levels is a matter of fundamental importance for the Province. The Service Provider will not agree or purport to agree with any Client, Stakeholder or other Person, whether in its own right or purportedly as agent for and on behalf of the Province, to amend, change or modify in any manner any of the Service Levels without the Approval of the Province.

8.5 Review and Changes to Service Levels.

The Parties acknowledge and agree that Service Levels are intended to be comprehensive, but not all inclusive, and accordingly, it is the intention of the Parties that during the Term the Parties may agree to different or additional Service Levels in respect of any of the Services. On an annual basis during the Term, and pursuant to the Governance Process, the Parties will jointly review the following:

(a) the then-current Service Levels;

(b) generally available information indicating industry-wide improvements in delivery of substantially similar services (including any available Benchmarker's reports commissioned in accordance with Article 9 (*Benchmarking*)); and

(c) improved performance capabilities, including those associated with advances in technology and processes used to provide the Services.

On the basis of such review, the Parties will discuss and agree upon whether any of the Service Levels will be adjusted. Any such adjustment will be subject to the mutual agreement of the Parties in accordance with the Governance Process, or as a Change Order through the Change Order Process. Any such adjustments, whether agreed to by the Parties in writing and signed by both Parties through the Governance Process, or whether through a Change Order pursuant to the Change Order Process, will be and be deemed to be an amendment to the Service Levels contained in **Schedule 11** *(Service Levels)* of this Agreement.

8.6 Monitoring.

From and after the Hand-Over Date, the Service Provider will establish and maintain in place, at all times, appropriate policies and procedures to monitor and evaluate the achievement of the Service Levels during the applicable measurement periods, including the maintenance of a service level log in order to permit the Service Provider, and the Province (as applicable), to:

(a) evaluate Achieved Service Levels;

(b) satisfy the reporting obligations under this Agreement;

(c) respond to, or to assist the Province in responding to, inquires from Stakeholders, the Ministry or any Clients of the Services regarding the Service Provider's performance of the Services;

(d) enable the Province to report publicly on the achievement or non-achievement of the Service Levels by the Service Provider in accordance with the Province's Policy, as such Policy may be amended from time to time; and

(e) confirm and verify Achieved Service Levels in respect of any Service Level from time to time upon reasonable notice.

8.7 Service Level Reports.

From and after the Hand-Over Date, and without limiting the application of Section 8.6 *(Monitoring)*, the Service Provider will prepare and maintain records and reports summarizing its Achieved Services Levels and providing the particulars of any failure of the Service Provider to meet a Service Level, organized by Service type (to the extent possible) and in such form and content as the Province may require. For greater clarification, any reports regarding the failure of the Service Provider to meet a Service Level will include detail regarding the particulars of the failure, a description of the measures taken or to be taken by the Service Provider to rectify and remedy the failure, and the timeline in which such measures were or are expected to be taken by the Service Provider, in order to allow the Province to:

(a) evaluate the consequence of such failure;

(b) communicate with or respond to the applicable Province Clients or Stakeholders that received the Service that failed to meet such Service Level; and

(c) cooperate with the Service Provider to rectify and remedy the consequence of such failure and to prevent future failures to meet such Service Level.

The Service Provider will provide such reports to the Province on a monthly basis and in accordance with applicable reporting requirements set out in **Schedule 21** *(Reporting Requirements)*, unless sooner requested by the Province from time to time. The Service Provider will also provide the Province with immediate notice of each material failure to meet a Service Level in accordance with the provisions of Section 8.8 (*Problem Alert and Escalation Procedures*).

8.8 Problem Alert and Escalation Procedures.

In order to facilitate the ability of the Parties to quickly address, mitigate or otherwise deal with an event, occurrence, error, deficiency, defect, interruption, malfunction or other similar matter with respect to the Services, or any other System or service provided by a Subcontractor or any other Person which is related to or otherwise impacts the Services, and which the Service Provider reasonably believes could have a material adverse effect on the delivery of the Services or could result in the Service Provider failing to meet a Service Level (each a "**Problem**"), the following provisions will apply:

(a) from and after the Hand-Over Date, the Service Provider will develop, implement, maintain and comply with Problem alert, escalation, and management procedures, which may be amended by the Parties through the Governance Process from time to time (the "**Problem Management Procedures**");

(b) if the Service Provider becomes aware of a Problem, then the Service Provider will immediately notify the Province of the Problem or, to the extent that such immediate notice is not possible, as soon as possible, by providing the Province with the particulars of the Problem;

(c) the Service Provider will treat the Problem as a priority, will work diligently to avert or minimize any adverse effect that the Problem may cause, and will deal with the Problem in accordance with the Problem Management Procedures;

(d) upon the occurrence of any Problem, the Service Provider will perform a root cause analysis in respect thereof as soon as practicable, and in any event, within any times required pursuant to the Problem Management Procedures, for purposes of identifying the cause of such Problem, and in order to assist the Service Provider in developing and implementing a proposal or workaround solution for correcting the Problem, and implementing improved processes to detect and avoid similar Problems in the future;

(e) the root cause analysis and proposal will be completed by the Service Provider as part of the Services at no additional cost to the Province;

(f) for greater clarification, and for purposes of this Section, any Problems of Subcontractors and Suppliers will be deemed to be Problems of the Service Provider; and

(g) the Service Provider will review each root cause analysis with the Province, monthly (or more frequently as may be requested by the Province from time to time) to monitor Service Provider's corrective and remedial actions (including detective and preventive actions).

For greater certainty, the Service Provide will not be required to perform a root cause analysis as described in Subsections 8.8(d), 8.8(e) and 8.8(g), in connection with a Problem in respect of systems owned or controlled by third parties (other than Subcontractors and Suppliers) for which the Service Provider has no control.

8.9 Service Level Failures.

The Service Provider's failure to meet any Service Level Agreement will be governed by the provisions of **Schedule 12** (*Service Level Failures*). The provisions of Appendix 11-C of **Schedule 11** (Service Levels) and **Schedule 12** (*Service Level Failures*) provide only partial compensation for the damage that may be suffered by the Province as a result of the Service Provider's failure to meet any Service Level Agreement. Accordingly, payment or application of any Service Level Credit pursuant to the provisions of Appendix 11-C of **Schedule 11** (Service Levels) and **Schedule 12** (*Service Level Failures*) is without prejudice to any entitlement that the Province may have to damages or other remedies under this Agreement, at law or in equity, including injunctive relief (to the extent available), as well as to the following:

(a) the removal of the Service in respect of which there was a failure to meet the applicable Service Level Agreement from the Services to be provided by the Service Provider pursuant to this Agreement, and an appropriate consequential reduction in the applicable portion of the Fees pursuant to the Change Order Process;

(b) the taking by the Province of all action necessary or desirable to correct, rectify and remedy such failure and the resulting consequences at the cost of the Service Provider including, without limitation, procuring or otherwise obtaining Services or goods from any alternative service providers or suppliers, and setting-off the cost of all such action and of the amount of all damages or loss suffered by the Province as a result of such failure against the Fees otherwise payable by the Province to the Service Provider; or

(c) a claim by the Province against the Guarantors under the Guarantees.

A failure to meet a Service Level Agreement which does not give rise to a Service Level Termination Event will not give rise to a right of the Province to terminate this Agreement, but will give rise to rights and remedies of the Province in respect of defaults generally in accordance with this Agreement including, without limitation, the provisions of this Section and the right to Service Level Credits in accordance with the provisions of **Schedule 12** (*Service Level Failures*).

ARTICLE 9 – BENCHMARKING

9.1 Benchmarking.

The Province may require benchmarking comparisons of any one or more of the Fees or the Service Levels to be performed (each, a "**Benchmarking**"), in which case the following will apply:

(a) the Benchmarking will not be performed more frequently than once in any two consecutive Contract Years, and the first Benchmarking will not be performed before April 1, 2012;

(b) the Service Provider will cooperate with the Province in connection with any such Benchmarking in the manner contemplated in Section 9.2 (*Benchmarking Cooperation*);

(c) the third party consultant performing the Benchmarking (the "**Benchmarker**") will be selected and engaged by the Province and the Service Provider jointly. If the Province and the Service Provider are not able to agree on the selection of the Benchmarker, then the matter will be a Dispute and will be settled in accordance with Article 27 *(Dispute Resolution)*;

(d) except as set forth in paragraph (g) below, the costs of the Benchmarker will be shared equally between the Province and the Service Provider;

(e) as a condition to its engagement, the Benchmarker will execute a Non-Disclosure Agreement;

(f) the Benchmarking will be a comparison of any one or more of the Service Levels and the Fees with the same or similar comparators of other entities receiving similar services, with appropriate adjustments being made where quantities or circumstances differ; and

(g) the Province will be entitled to perform one (1) Benchmarking at any time after the Province gives notice, or is deemed to have given notice, to the Service Provider under Sections 2.6 (*Renewal Notice*) or 2.7 (*Renewal Negotiations*) that the Province does not intend to renew this Agreement, at the sole cost of the Province.

9.2 Benchmarking Cooperation.

Unless the Parties otherwise agree, the Province will, with the Service Provider's concurrence, determine the scope, methodology, relative comparisons and execution of each Benchmarking. The Service Provider will cooperate in the Benchmarking studies by providing information requested in relation to the Benchmarking, and in particular, the Service Provider will provide:

(a) the Benchmarker (and will ensure that its Subcontractors provide, either directly to the Benchmarker or to the Service Provider), all necessary information, documents and assistance as may be reasonably required for the Benchmarker to perform the Benchmarking; and

(b) the Benchmarker with reasonable access to the Service Provider's performance data and, where necessary, access (which may be supervised) to the Service Provider's performance measurement tools to independently verify reported Achieved Service Levels.

9.3 Benchmarker's Report.

Each Party will receive a copy of the Benchmarker's report and will have an opportunity to review the same and make submissions to the other Party with respect to the findings contained in the Benchmarker's report prior to any adjustments to the Services, the Service Levels or the Fees as a result of such Benchmarking. Any such adjustments will require the mutual written agreement signed by the Parties in accordance with the Governance Process or through the Change Order Process, as applicable. If the Benchmarking results show that the Service Levels reported by the Service Provider are materially different than actual performance, then the Benchmarker will use actual performance as the basis of comparison.

9.4 Client Satisfaction.

The Service Provider will cooperate with the Province to obtain information concerning the levels of Stakeholder and Client satisfaction with the Services, including by the following:

(a) assisting the Province to survey Stakeholders and Clients as to their level of satisfaction with the performance of the Services, which surveys will be initiated and undertaken by the Service Provider only upon the direction and Approval of the Province (and the Approval of the Province will include Approval as to the format, content and process for such survey to be conducted by the Service Provider); and

(b) tracking performance levels and Client complaints as well as the response to and handling of such complaints.

The results of any customer satisfaction surveys will be reviewed by the Parties through the Governance Process. If the results of the survey indicate a failure or perceived failure to meet applicable Service Levels, or a decrease in the level of Client satisfaction, then within two (2) months of receipt of the survey results, the Service Provider will design and propose a remedial plan (in consultation with the Province through the Governance Process) to prevent reoccurrence of the problem and to increase Client satisfaction of the applicable parties. The Service Provider will implement the same in accordance with the Change Order Process.

ARTICLE 10 – BRANDING AND COMMUNICATIONS

10.1 Use of Province Marks.

In respect of the use or display by the Service Provider of any trade-marks, official marks, business names, trade names, domain names, trading styles, logos, or other distinguishing marks of the Province, whether registered or unregistered (each a "**Province Mark**"), the Parties agree as follows:

(a) prior to any display or use of a Province Mark by the Service Provider in the performance of the Services, the Service Provider will obtain the Approval of the Province;

(b) subject to Section 10.2 (*Brand Use*), any display or use of the Province Marks by the Service Provider will only be for the duration of the Term, on a non-exclusive basis, and only for the purposes of providing the Services;

(c) the Service Provider will use the Province Marks only in accordance with this Agreement and in the manner expressly permitted in writing by the Province and provided that:

(i) the character and standards of quality of the wares and Services in respect of which the Province Marks may be used by the Service Provider are as set out in **Schedule 15** *(Conditions of Use of Province Marks)*,

(ii) such display or use of the Province Marks is in accordance with the provisions of **Schedule 15** *(Conditions of Use of Province Marks)*, appropriate legends and the Province Policies including, without limitation, any policies established or enforced by the Province's Public Affairs Bureau, notice of which will be given to the Service Provider, and all usage guidelines and restrictions as reasonably prescribed from time to time by the Province in respect thereof, or in accordance with other express permissions granted by the Province, and

(iii) the Service Provider may not register or carry on business under a business name that contains any of the Province Marks unless specifically Approved by the Province;

(d) upon Termination of this Agreement, the Service Provider:

(i) will immediately cease any and all use of the Province Marks,

(ii) will discontinue the provision of all products and Services in association with the Province Marks, and

(iii) will not, and will ensure that its Affiliates do not, thereafter use the Province Marks or any trade-mark or trade name confusingly similar to the Province Marks;

(e) during and after the Term the Service Provider will not, and will ensure that its Affiliates do not, challenge the validity of the Province Marks or the Province's ownership of the Province Marks;

(f) any and all goodwill that is or may be acquired from the use of a Province Marks by the Service Provider or its Affiliates will vest in and be, and be deemed to be, the property of the Province;

(g) the Province is and will remain the owner of the Province Marks, and the Service Provider will not obtain any rights in or to the Province Marks other than the right to use the Province Marks in accordance with the provisions of this Section 10.1 (*Use of Province Marks*);

(h) at the request of the Province, the Service Provider will provide the Province with samples of the Service Provider's use of the Province Marks; and

(i) the Service Provider will not use or register any Province Marks or any marks confusingly similar to the Province Marks except as expressly Approved by the Province under or in accordance with the terms of this Agreement.

10.2 Brand Use.

The Service Provider will provide the Services under the branding of the Province Marks set forth in **Schedule 16** (*Conditions of Use of Province Marks*), but subject to the provisions of Section 10.1 (*Use of Province Marks*), as the same may be changed from time to time by the Province pursuant to the Change Order Process, all of which is hereby Approved by the Province. Such Approval by the Province will not restrict the Province's right to use any such Province Marks, or to license the same to any other Person, or use or license any other Province Marks similar thereto.

10.3 Service Provider Marks.

Except as may otherwise be expressly required pursuant to Applicable Law, or as may be Approved by the Province, the Service Provider will not use or display any of the Service Provider's trade-marks, official marks, corporate names, business names, trade names, domain names, trading styles, logos, or other distinguishing marks (each a "**Service Provider Mark**") together or in conjunction with any Province Marks. Notwithstanding any such requirement pursuant to Applicable Law, or Approval by the Province, the Province will not obtain any rights in or to the Service Provider Marks, and any and all goodwill that is or may be acquired from the such use of a Service Provider Mark by the Service Provider will vest in and be, and be deemed to be, the property of the Service Provider.

10.4 Publicity.

The Service Provider will submit to the Province all advertising, written sales promotion, press releases, public notices and any and all other publicity matters or materials relating to this Agreement or the transactions contemplated by this Agreement, or in which the Province's name or any Province Marks are mentioned or language from which connection with the Province's name or any Province Marks may be inferred or implied (the "**Publicity Materials**"). The Service Provider will not publish or use any Publicity Materials without the prior consultation with and Approval of the Province, which Approval

will not be unreasonably withheld. Notwithstanding the foregoing, the Service Provider may include the Province's name and a factual description of the work performed under this Agreement only:

(a) on employee bulletin boards;

(b) in internal business planning documents;

(c) for account referral purposes when Approved by the Province;

(d) whenever otherwise required by reason of legal, accounting or regulatory requirements; and

(e) in proposals where such proposal language has been Approved by the Province.

In addition, no disclosure, including press releases, will be made by the Service Provider regarding any aspect of the Services or the Province without the Approval of the Province. In the event of potentially negative publicity or other potentially adverse effects upon the Service Provider in connection with the Services or this Agreement, the Service Provider will be entitled to respond to the same provided that it does so in consultation with the Province, and that the Province is given the opportunity to first Approve the contents of any such response insofar as it relates to the Province, the Services or this Agreement.

10.5 Stakeholder Communications.

Unless specifically provided otherwise in this Agreement, all communications by the Service Provider to the Stakeholders will be in accordance with the Communication Plan and other processes and procedures as set forth in **Schedule 17** *(Communications Plan and Processes)*.

10.6 Adverse Impact Notice.

The Service Provider will provide the Province with prior notice (which need not be in writing), if possible, of events with respect to the Service Provider and its Affiliates that the Service Provider anticipates will become public and could reasonably be expected to adversely impact the Province or the relationship between the Parties, or be covered negatively in any North American media. The Service Provider's obligation to provide such notice is subject to the provisions of Applicable Laws, including securities laws applicable to the Service Provider and its Affiliates, and to the confidentiality obligations of the Service Provider and its Affiliates. Where it is not possible for the Service Provider to provide prior notice to the Province, the Service Provider will notify the Province as soon as possible.

ARTICLE 11 – RELATIONSHIP MANAGEMENT AND HUMAN RESOURCES

11.1 Governance.

During the Term, the relationship of the Parties (including the mechanisms by which they will manage this Agreement, each with the other) will be expressly governed by the provisions of this Article 11 (*Relationship Management and Human Resources*) and the processes, procedures and provisions set forth in the governance structure attached as **Schedule 18** *(Governance)*, as **Schedule 18** *(Governance)* may be jointly amended from time to time by the Parties in accordance with the terms of this Agreement.

11.2 Cooperation of the Parties.

Each Party will cooperate with the other, in good faith, in the performance of its obligations under this Agreement. In connection therewith, each Party will make available, as reasonably requested by the other

Party, such management decisions, information, approvals and acceptances such that the provision of the Services under this Agreement may be accomplished in a proper, timely and efficient manner and in accordance with the processes and procedures set forth in this Agreement. Unless specifically provided otherwise in this Agreement, where an agreement, approval, acceptance or consent of the other Party is required by any provision of this Agreement, then such action will not be unreasonably withheld or delayed, having regard to all of the surrounding circumstances. The Parties agree that it will not be considered reasonable for any requested response time for an agreement, approval, acceptance or consent from the Province to be less than five (5) Business Days except in extraordinary circumstances clearly demonstrated in writing by the Service Provider. Notwithstanding the foregoing, nothing in this Section 11.2 (*Cooperation of the Parties*) will in any manner relieve the Service Provider from performing its obligations, or delivering the Services, as contemplated under, and in accordance with, the terms of this Agreement.

11.3 Power and Authority of the Service Provider.

Except as otherwise set forth in this Agreement, and subject to the terms of this Agreement, the Service Provider will have the power and authority to take such actions as it deems to be prudent, necessary or advisable to perform the Services in accordance with the terms and conditions set forth in this Agreement. Notwithstanding the foregoing, the Service Provider will not take any action required by this Agreement, if such action is:

(a) subject to the Approval of the Province, without having received such Approval; and

(b) subject to consultation with the Province, without having undertaken such consultation.

For greater clarification, no such Approval or consultation will in any manner relieve the Service Provider from performing its obligations, or delivering the Services, as contemplated under, and in accordance with, the express terms of this Agreement, nor will such Approval or consultation have any effect on the allocation of risk to the Service Provider as a result of the covenants, obligations and requirements of the Service Provider under the terms of this Agreement.

11.4 Province's Right to Issue Directives.

The Province may, from time to time, at the Service Provider's request or at the Province's own initiative, issue written directives and instructions and establish written policies and procedures governing the duties and obligations of the Service Provider relating to the Services (including with respect to confidentiality, privacy and security), in order to cause the Service Provider to comply with the Province's Policies or business requirements in the performance of the Services (each a "**Directive**"), in which case, the following provisions will apply:

(a) the Directives will be subject to the Change Order Process and will be deemed to be a Mandatory Change Request;

(b) the Province will, through the Governance Process, provide the Service Provider with timely written notice of the Directives;

(c) the Service Provider will at all times act in accordance with the Directives that it has so received from the Province, provided that the Directives do not oblige the Service Provider to perform any duty or obligation not provided for or otherwise contemplated under this Agreement, and do not have the effect of causing the Service Provider to be in breach of any Applicable Laws;

(d) the Province will provide the Service Provider with a reasonable period of time to comply with a Directive, having regard to all of the surrounding circumstances, the nature of the Directive, and the requirements of the Change Order Process (including, without limitation, the Mandatory Changes), it being acknowledged by the Parties that the nature of some Directives may necessitate immediate compliance, in which case, the Service Provider will comply with the Directive as promptly as practicable; and

(e) subject to the requirements of the Change Order Process (including, without limitation, the Mandatory Changes), the failure or refusal of the Service Provider to comply with a Directive that it has received from the Province within the times required pursuant to this Agreement, and in accordance with the provisions of this Section, may constitute a Material Breach under the provisions of Section 28.1 *(Service Provider Material Breach)*.

11.5 Province Approval.

In connection with the Services performed by the Service Provider under this Agreement, and unless specifically provided otherwise in this Agreement, the Service Provider will not undertake any matter outside of the scope of the Services contemplated under this Agreement throughout the Term, and will not undertake any of the following matters without the prior Approval of the Province:

(a) any financing or borrowing from a Person other than from an Affiliate of the Service Provider, and other than trade credit in the ordinary course, that could cause or permit (and the Service Provider will not otherwise cause or permit) the creation or maintenance of any security interest, charge, pledge or other encumbrance on the rights of the Service Provider under this Agreement or on any assets used in the provision of Services by the Service Provider or its Affiliates (other than leased equipment from arm's length third parties);

(b) those matters specifically identified in this Agreement as requiring the Approval or other authorization or consent of the Province;

(c) making or agreeing to make any capital expenditure on behalf of the Province; or

(d) retaining legal counsel on behalf of the Province with respect to any matter involving any Service, or initiating or responding to any legal, regulatory or other proceeding on behalf of the Province, or settling any Claim prosecuted by or against the Province arising from a legal or regulatory proceeding regarding any Service.

If the Approval of the Province is required pursuant to this Agreement, then except as specifically provided otherwise in this Agreement, the Service Provider will deliver written notice to the Province through the Governance Process, setting out the particulars of the matter and requesting the Approval of the Province, and setting forth the reasonable time period in which a response is required, and if applicable, the implications of not responding within that time period. The Parties agree that it will not be considered reasonable for the requested response time to be less than five (5) Business Days except in extraordinary circumstances clearly demonstrated in the Service Provider's notice. The Province will use reasonable efforts to respond to any request from the Service Provider for the Approval of the Province within a reasonable period of time, having regard to all of the surrounding circumstances. Except as specifically provided otherwise in this Agreement, the failure of the Province to respond to a request for an Approval during the period suggested by the Service Provider will not result in any liability on the part of the Province to the Service Provider or be deemed to constitute the Approval of the Province by acquiescence or otherwise. Where the Province delays in providing such response to the Service Provider in circumstances where the request for the Approval from the Service Provider expressly sets forth the

consequences of not responding within the required time period, then the Service Provider will not be responsible for any breach by the Service Provider of its obligations under this Agreement where the same are directly attributable to the delay of the Province in providing such response.

11.6 Key Positions.

Recognizing the importance of executive continuity to the ongoing success of the Parties' relationship, and to the successful performance of the Services under this Agreement, the Service Provider will use all reasonable efforts to minimize turnover of personnel in the Service Provider positions, as more particularly described in **Schedule 19** (*Key Positions*) (the "**Key Positions**"), as may be changed from time to time by the Parties in accordance with this Section 11.6 (*Key Positions*) and Section 11.7 (*Changes in Key Positions*). At all times during the Term, the Service Provider will ensure that the Key Positions are appropriately staffed and available as may be necessary to ensure the continuous and uninterrupted provision of the Services. Subject to Subsection 11.7(a) and (b) (*Changes in Key Positions*), the foregoing will constitute a material obligation for purposes of Section 28.1 (*Service Provider Material Breach*). The Parties may, from time to time through the Governance Process, re-designate the positions that constitute Key Positions.

11.7 Changes in Key Positions.

The Province has entered into this Agreement in reliance upon and with the expectation that the personnel in the Key Positions will be engaged in the provision of the Services to the Province, and with the expectation of reasonable continuity in the Key Positions. Accordingly, the Service Provider will implement personnel changes in the Key Positions in accordance with the following:

(a) the Service Provider may replace a person holding a Key Position, or appoint a new person to fill a vacancy caused by the resignation or other departure of a person holding a Key Position, provided that:

(i) the Service Provider does not transfer any individual in a Key Position on a lateral basis without promotion to another project or Affiliate of the Service Provider without the prior Approval of the Province,

(ii) the Service Provider provides the Province with reasonable prior written notice thereof, if possible, together with relevant information regarding the background qualifications of the person that the Service Provider wishes to appoint to the Key Position, and such other information regarding the qualifications of such person as the Province may request,

(iii) the Service Provider provides the Province with the opportunity to interview the person that the Service Provider wishes to appoint or hire into the Key Position prior to the final decision being made in respect of such appointment or hire, and the Service Provider considers comments from, and consults with, the Province in respect of such interview,

(iv) the Service Provider obtains the Approval of the Province pursuant to the provisions of **Schedule 19** *(Key Positions)* in respect of any candidate that will replace the following: President, EDS Advanced Solutions Inc.; Strategic Transformation and Mainframe Services (STMS) Lead; Managed Services Lead; and Security & Privacy Lead of the Service Provider, and

(v) the Service Provider provides the Province with a transition plan for the replacement of the incumbent with a new person in the Key Position;

(b) in the event of an extended or unexpected absence of the incumbent in a Key Position, the Service Provider will forthwith advise the Province of such absence, and the Parties will consult with each other as to the appropriate steps to be taken by the Service Provider in respect of such absence; and

(c) any person assigned to or otherwise placed in a Key Position will have qualifications or experience appropriate to the position which will be at least equivalent to the qualifications and experience of the initial person in such Key Position unless otherwise Approved by the Province, and such person will be suitably trained and transitioned to the Key Position.

11.8 Key Position Failures.

At any time, and from time to time, during the Term, the Province or the Service Provider may by notice (which may be oral) to the other, declare that a Key Position has failed to satisfactorily perform the duties of such position. The parties will promptly discuss such concerns, and where the Parties cannot agree on an appropriate course of action in respect thereof, then such issue will be elevated to the Joint Executive Committee for consideration, or such other discreet channels of communication as may be appropriate under the circumstances. Where the Joint Executive Committee provides any direction, including removal of such person, then the Service Provider will promptly adhere to and implement such direction at the Service Provider's sole cost.

11.9 General Principles Regarding Personnel.

At all times during the Term, the Service Provider will employ sufficient personnel of the Service Provider, including both employees and independent contractors of the Service Provider (collectively, "**Personnel**"), and will ensure that sufficient personnel are employed by its Subcontractors (collectively, "**External Personnel**"), to perform the Services in accordance with Service Levels and the other terms and conditions of this Agreement. The following provisions will apply with respect to the Personnel and the External Personnel:

(a) unless specifically provided otherwise in this Agreement, the Service Provider will be responsible for the management and supervision of, and for the acts, omissions, performance of, and damage caused by the Personnel and External Personnel in the performance of the Services;

(b) the Service Provider will ensure that the use of all Foreign Employed Individuals in the performance of the Services will comply with the Privacy Obligations applicable thereto;

(c) the Service Provider will ensure that the Personnel and External Personnel performing the Services:

(i) possess a degree of skill and experience appropriate to the tasks to which they are assigned and the performance and Service Levels which they are required to achieve,

(ii) receive appropriate training (including quality training courses, refresher courses and retraining programs) for the performance of the Services and compliance with the confidentiality provisions and Privacy Obligations in the Agreement,

(iii) perform the Services to the standards set out in this Agreement, and

(iv) strictly comply with the privacy, security and confidentiality provisions set forth in the Privacy Obligations;

(d) where given a Directive by the Province pursuant to Section 11.4 (*Province's Right to Issue Directives*), or where otherwise necessary, appropriate or prudent to do so given the nature of the Services or of the Province Confidential Information being accessed, used or disclosed, the Service Provider will conduct appropriate background checks with respect to the applicable Personnel, and will contractually require Subcontractors to do the same with respect to the applicable External Personnel, prior to such personnel commencing to provide the Services;

(e) subject to the terms of the Master Transfer Agreement and unless specifically provided otherwise under this Agreement, the Service Provider will be solely liable and responsible (to the exclusion of the Province) for all costs, expenses, liabilities or claims, whenever incurred, relating to:

(i) salaries and other compensation payable to its Personnel,

(ii) labour relations proceedings or orders, grievances, arbitration proceedings or unsatisfied arbitration awards relating to its Personnel,

(iii) strikes or other actions due to labour disputes involving its Personnel, and

(iv) complaints, claims, decisions, applications, orders or prosecutions under any employment or labour standards, occupational health and safety, workers' compensation, pay equity, employment equity and human rights legislation relating to its Personnel,

regardless of the time that the matter or event giving rise to any such costs, expenses, liability or claims arises or occurs, and for greater clarification, unless provided otherwise under the terms of the Master Transfer Agreement or this Agreement, none of such costs, expenses, liabilities or claims referred to in this paragraph (e) above will be subject to reimbursement by the Province to the Service Provider;

(f) the Service Provider will deal with its Subcontractors in such a manner that the Province will have no liability resulting from the failure of the Subcontractors to meet the same responsibilities and payment obligations as described in paragraph (e) above with respect to the External Personnel, subject to the terms of the Master Transfer Agreement, and for greater clarification, none of such costs, expenses, liabilities or claims contemplated in this paragraph (f) will be subject to reimbursement by the Province to the Service Provider or to the Subcontractors;

(g) the Service Provider will comply at all times with all applicable collective agreements and all applicable employment standards, occupational health and safety, workers' compensation, human rights legislation, and other Applicable Laws relating to its Personnel, will cause each Subcontractor to comply with the same as applicable to the External Personnel of such entities, subject to the terms of the Master Transfer Agreement, and will deal with all Subcontractors in such a manner that the Province will have no liability resulting from any failure of the Subcontractors to so comply with such responsibilities and obligations with respect to the External Personnel; and

(h) except as expressly provided otherwise in this Agreement or in the Master Transfer Agreement, the Service Provider will be solely liable and responsible for, to the exclusion of the Province, all costs arising from or otherwise relating to the termination by the Service Provider of any Personnel, and will ensure that the Province has no liability for the termination by any Subcontractor of any External Personnel, and the Service Provider and the Subcontractors will not be reimbursed by the Province for any such costs, expenses, claims or liabilities.

11.10 Administrator.

The Province shall act as the administrator of the Agreement in connection with the Broader Public Sector's purchase of Services under this Agreement and in accordance with the provisions of Schedule 5 (*Special Terms*).

ARTICLE 12 – SUBCONTRACTORS

12.1 Responsibility for Subcontractors.

The Service Provider is the general contractor for the Services under this Agreement and remains responsible for all of its obligations under this Agreement, regardless of whether the Service Provider relies upon any Subcontractor to any extent. Subject to the terms of this Agreement:

(a) the Service Provider's use of Subcontractors for any of the Services will in no way increase the Service Provider's rights or diminish the Service Provider's liabilities to the Province with respect to this Agreement;

(b) the Service Provider's rights and liabilities under this Agreement with respect to the Province will be as though the Service Provider had itself performed such Services;

(c) the Service Provider will be liable for any defaults or delays caused by any Subcontractor in connection with the Services as if such defaults or delays were caused by the Service Provider; and

(d) the Service Provider will be fully liable for all actions and omissions of the Subcontractors in the performance of the Services.

If a Subcontractor breaches a Subcontract, or is alleged to have breached a Subcontract, which could have a material affect on the delivery of the Services or the performance of the Service Provider's obligations under this Agreement, then the Service Provider will notify the Province in writing and provide the Province with such information relating to the alleged breach as the Province may request.

12.2 Inconsistent Subcontract Terms.

The terms of this Agreement will in all events be binding upon the Service Provider notwithstanding, and without regard to:

(a) the existence of any inconsistent or contrary terms in any agreement between the Service Provider and any Subcontractor, subject to Section 12.7 (Assigned Contracts); and

(b) the fact that the Province may have directly or indirectly been given or otherwise received notice of the existence of any inconsistent or contrary terms in any agreement between the Service Provider and any Subcontractor.

12.3 General Contract Terms (Subcontractors).

Subject to Section 12.8 (*Material Subcontractors*), all Subcontracts entered into by the Service Provider with Subcontractors will not include any terms or provisions that are inconsistent with, or contrary to, the terms and conditions of this Agreement, and all such Subcontracts will include the following provisions:

(a) a requirement that the Subcontractor adhere to the applicable obligations that:

(i) are expressly required by this Agreement to be imposed upon the Subcontractor, and

(ii) are otherwise required for the Service Provider to perform its obligations to the Province under this Agreement including, without limitation, the Service Levels, confidentiality obligations, intellectual property provisions, Privacy Obligations, and reporting, audit and access rights and requirements;

(b) assignment or licensing of Intellectual Property Rights to the Service Provider in respect of any deliverables created in such relationship, and waiver of moral rights in respect of the same, to the extent required by the Service Provider to comply with its obligations to the Province under this Agreement;

(c) obligations regarding compliance with Applicable Laws, including source deductions and remittances (for taxes, workers compensation and similar requirements);

(d) termination rights consistent with the terms of this Agreement;

(e) to the extent possible, assignment rights to the Province or the Alternative Service Provider upon the early termination or expiry of this Agreement in accordance with its terms, without any further consent from the Subcontractor or any additional, accelerated or other similar payments having to be made; and

(f) any other provisions necessary for the Service Provider to fulfill its obligations under this Agreement.

The foregoing will not apply with respect to any Assigned Contracts to the extent set forth in Section 12.7 (*Assigned Contracts*).

12.4 Subcontractor Monitoring.

During the Term, the Service Provider will:

(a) monitor the performance of Subcontractors and promptly address and remedy any performance issues or disputes with Subcontractors in such a manner which has no adverse impact on the nature, quality or delivery of the applicable Services; and

(b) ensure that contingency plans are devised for the possibility of a Subcontractor failing to perform, needing to be replaced, or terminating the Subcontract with the Service Provider before the Termination of this Agreement.

12.5 Non-Disclosure Documents.

Unless otherwise Approved by the Province, all External Personnel of Access Subcontractors (including all External Personnel of any Affiliates of the Service Provider who may have access to, or use or

disclosure of, Personal Information) will be required to execute documents directly with the Service Provider binding such External Personnel to confidentiality and non-disclosure agreements as required by the Province and in a form Approved by the Province, all as more particularly described in the Privacy Obligations contained in **Schedule 24** *(Privacy Obligations)* (the "**External Personnel Agreements**"). The Service Provider will not disclose or provide access to any Personal Information to any such External Personnel until such External Personnel have entered into an External Personnel Agreement.

12.6 Confidentiality Breaches.

Unless specifically provided otherwise under this Agreement, any breach of the confidentiality obligations set forth in this Agreement by a Subcontractor, or any External Personnel of such Subcontractor, will be deemed to constitute a breach of the confidentiality provisions of this Agreement by the Service Provider. In the event of any breach of confidentiality obligations by a Subcontractor, or any External Personnel of a Subcontractor, the Parties agree as follows:

(a) in the event that either Party discovers that a breach of confidentiality by a Subcontractor or any External Personnel of a Subcontractor has occurred, it will promptly notify the other Party in writing;

(b) the Service Provider will take all steps necessary to remedy or to have remedied such breach;

(c) the Service Provider will develop and inform the Province of any remedial plans to remedy or otherwise deal with such breach;

(d) if the Province Approves such remedial plan, and the Service Provider carries out the remedial plan, then the Province will not be entitled to terminate this Agreement solely on the basis of the Subcontractor's breach of confidentiality;

(e) if the Service Provider does not carry out the remedial plan, then such failure to carry out the remedial plan will constitute a Material Breach for the purposes of Subsection 28.1(k) *(Service Provider Material Breach)*; and

(f) if the Province

(i) determines, in its reasonable opinion, that the breach of confidentiality obligations is material; or

(ii) does not Approve such remedial plan, acting reasonably,

then such breach will constitute a Material Breach for purposes of Subsection 28.1(k) (*Service Provider Material Breach*).

12.7 Assigned Contracts.

For purposes of this Agreement, and in respect of those Subcontracts that are Assigned Contracts, the following provisions will apply:

(a) the Service Provider will enforce the existing provisions in such Assigned Contracts;

(b) the Service Provider will not, without the Province's Approval, reduce or eliminate existing provisions with respect to confidentiality, privacy and security;

(c) the Service Provider will use reasonable efforts to expand the confidentiality, privacy and security provisions of such Assigned Contracts to be in conformance with the requirements of this Agreement in respect thereof;

(d) the failure of an Assigned Contract to include provisions required by this Agreement to be included in a Subcontract, including the following, will not constitute a breach of this Agreement:

(i) provisions corresponding to the provisions of this Agreement that are required to be flowed down to Subcontractors,

(ii) any Privacy Obligations applicable to Subcontractors, including a requirement that External Personnel of the Subcontractor execute an External Personnel Agreement, or

(iii) in the case of an Assigned Contract that is a Material Subcontract, the provisions required to be included by Section 12.9 (*Additional Material Subcontract Terms*),

(e) when renewing or renegotiating such Assigned Contracts at the end of their respective current terms (and prior to any renewals or extensions thereof), the Service Provider will amend the terms to comply with the provisions of this Agreement; and

(f) as a condition of any renewal or renegotiation of any Assigned Contract at the expiry of its Term, or to any extension of an existing term of any Assigned Contract, and unless otherwise Approved by the Province (although any such Approval will not, and will not be deemed to, reduce any of the obligations of the Service Provider under the Privacy Obligations), the Service Provider will ensure that any such renewed, extended or renegotiated Assigned Contracts complies with the Privacy Obligations to the extent that the Privacy Obligations are applicable thereto, including the requirement that External Personnel of the Subcontractor accessing Personal Information execute an External Personnel Agreement.

Any breach of the confidentiality or the privacy and security provisions (if any) contained in the Assigned Contracts by Subcontractors will be deemed to constitute a breach of the confidentiality or the privacy and security provisions of this Agreement.

12.8 Material Subcontractors.

Any Subcontract entered into by the Service Provider for the performance of any part of the Services by a Subcontractor, where the Subcontractor meets the conditions or requirements set forth in **Schedule 20** *(Subcontractor Matters)* in respect thereof, will constitute a "**Material Subcontract**" to which the provisions of Section 12.9 (*Additional Material Subcontract Terms*), in addition to the provisions set forth in Section 12.3 (*General Contract Terms* (*Subcontractors*), will apply, but excluding therefrom any contracts that are Assigned Contracts.

12.9 Additional Material Subcontract Terms.

Unless consented to in writing by the Province, all Material Subcontracts entered into by the Service Provider will, in addition to the provisions set forth in Section 12.3 (*General Contract Terms* (*Subcontractors*), include the following provisions:

(a) provisions by which any Material Subcontractor who has or could have access to, use or disclosure of Personal Information in connection with the Services is bound to any applicable Privacy Obligations as identified in **Schedule 24** *(Privacy Obligations)*;

(b) provisions naming the Province as an intended third party beneficiary of the Material Subcontract and providing for the delivery by the Material Subcontractor of a certificate to such effect to the Province upon request;

(c) an agreement by both the Service Provider and the Material Subcontractor not to directly or indirectly assign the Material Subcontract to any Person without the Approval of the Province, not to be unreasonably withheld or delayed; and

(d) provisions entitling the Service Provider to terminate the Material Subcontract in response to a notice received from the Province under Section 12.13(a) (*Removal of Subcontractor*).

12.10 Extracts of Subcontracts.

During the Term of this Agreement, and at the request of the Province, the Service Provider will provide the Province with certificates signed by the Service Provider that have extracts of Material Subcontracts attached thereto, in a form sufficient for the Province to confirm the Service Provider's compliance with the obligations set forth in this Article 12 (*Subcontractors*). In connection therewith, the Service Provider will provide such certificate to the Province in respect of the Material Subcontracts described in the attached **Schedule 20** *(Subcontractor Matters)*, concurrently with the execution of this Agreement.

12.11 Consent to Use of Material Subcontractors.

The Service Provider will not use any Material Subcontractors in respect of the provision of any Services or other obligations performed under or in connection with this Agreement unless the Service Provider obtains the Approval of the Province, and for purposes hereof those Material Subcontractors described in **Schedule 20** *(Subcontractor Matters)* are hereby approved by the Province. Any request for Approval of a Material Subcontractor will include information regarding the components of the Services affected, the scope of the proposed Material Subcontract, the identity and qualifications of the proposed Material Subcontractor, whether the proposed Material Subcontractor is an Affiliate of the Service Provider, whether the proposed Material Subcontractor is a Canadian Entity, the foreign ownership (direct or indirect) of the proposed Material Subcontractor (if any), and the reasons for subcontracting the work in question.

12.12 Province Criteria for Material Subcontractors.

In considering a request for the Approval of a Material Subcontractor under the provisions of Section 12.11 (*Consent to Use of Material Subcontractors*), the Province will consider the reputation, financial stability, qualifications, applicable experience, ability, direct and indirect ownership, and availability of the Material Subcontractor, whether the Material Subcontractor who may have access to, or use or disclosure of Personal Information is a Canadian Entity, and the extent to which the Material Subcontractor could or would have access to, use or disclosure of any Personal Information, the purpose of such access, use and disclosure by (and by any External Personnel of) the Material Subcontractor. The Service Provider will not be required to provide to the Province any Subcontract (or draft Subcontract) with a Material Subcontractor (or proposed Material Subcontractor) in connection with a request for or to obtain the Province's Approval of the Material Subcontractor, except to the extent contemplated in Section 12.10 (*Extracts of Subcontracts*).

12.13 Removal of Subcontractor.

In the event that the Province determines, acting reasonably, that:

(a) the continued use of a Material Subcontractor will or could have a detrimental effect on the Province, and is therefore not in the best interests of the Province as a result of the Province having severed all other relationships with such Material Subcontractor due to the wilful misconduct, fraud or other forms of malfeasance by such Material Subcontractor; or

(b) the risk of a breach of the provisions of the *Freedom of Information and Protection of Privacy Act* is increased as a result of, but not limited to, an Access Subcontractor ceasing to be a Canadian Entity;

then the Province will give the Service Provider notice thereof (and specifying in detail the reasons therefor) through the Joint Executive Committee, requesting that such Material Subcontractor or Access Subcontractor be replaced. Promptly following receipt of such notice, the Service Provider will investigate the matters stated in the notice and discuss its findings with the Province through the Joint Executive Committee. If requested to do so by the Province (acting reasonably), the Service Provider will (within the timeframe specified by the Province after consultation with the Service Provider in respect of such timeframe) remove any access that the Material Subcontractor or Access Subcontractor may have to the Personal Information pending completion of the Service Provider's investigation and discussions with the Province. If, following such discussions with the Service Provider through the Joint Executive Committee, the Province reaffirms, acting reasonably, its request for the replacement of such Material Subcontractor or Access Subcontractor, then the Service Provider will, within ninety (90) days (or such different period of time as may be agreed to between the Parties through the Joint Executive Committee having regard to all of the surrounding circumstances) of such reaffirmation, replace such Material Subcontractor or Access Subcontractor with a new Material Subcontractor or Access Subcontractor of suitable qualifications, or will perform the applicable Services directly.

12.14 Other Business with Subcontractors.

Nothing contained in this Agreement will prohibit or otherwise restrict the Province from entering into agreements or other arrangements with any Subcontractor.

12.15 Suppliers.

The Service Provider may enter into contracts with Suppliers in respect of the Services (including for third party Software or for support or maintenance service) with such Suppliers as the Service Provider may select, provided that the Service Provider complies with any other applicable provisions of this Agreement regarding the use of Software in providing the Services. The following provisions will apply to contracts with Suppliers entered into by the Service Provider (other than contracts with Suppliers constituting Assigned Contracts) (it being understood that any Person who is given access to or use of Personal Information is an Access Subcontractor and not a Supplier for the purposes of this Agreement):

(a) all costs and expenses of such contracts with Suppliers will be the sole responsibility of the Service Provider, including any termination cost, penalties or other amounts payable in connection with such contracts;

(b) the Service Provider will ensure that the Suppliers have the required skill, qualifications and experience necessary to perform their obligations, and in the case of janitorial services, the Service Provider will retain bonded janitors only;

(c) the Service Provider will ensure that its Suppliers do not obtain access to Personal Information or Province Confidential Information by employing appropriate security policies, including, without limitation, a clean desk policy; and

(d) the Service Provider will not be relieved of any of its obligations in respect of the Services or under this Agreement as a result of any contracts with Suppliers, and the Service Provider will be responsible for all actions and failure to act of all of its Suppliers and the consequences thereof.

The Service Provider will monitor the performance of its Suppliers and will promptly address and remedy any performance issues or disputes in a manner which has no adverse impact on the nature, quality or delivery of the Services.

ARTICLE 13 – REPORTING AND ANNUAL OPERATING PLAN

13.1 Reporting Generally.

At all relevant times during the Term, the Service Provider will prepare or cause to be prepared, and will provide to the Province all reports and information required by the Province from time to time. The reporting requirements of the Province, which will be effective as and from the Hand-Over Date (and which excludes any reports or information to be provided by the Service Provider to the Province in connection with the Transition Services) is set forth in **Schedule 21** *(Reporting Requirements)*, and is subject to adjustment or amendment by the Parties through the Governance Process.

13.2 Annual Review of Reporting Requirements.

The Parties, through the Governance Process, will conduct an annual review of the then current reporting requirements under this Agreement and as set forth in **Schedule 21** *(Reporting Requirements)*, as the same may be adjusted or amended from time to time, and will consider any changes to the current reporting requirements as the Parties may determine to be appropriate or desirable.

13.3 Changes to Reporting Requirements.

The Parties acknowledge that the reporting requirements set forth in **Schedule 21** *(Reporting Requirements)* will evolve over the Term as a result of the addition of Services, changes made through the Change Order Process and otherwise. Subject to the provisions of **Schedule 21** *(Reporting Requirements)*, the Service Provider agrees that any changes to the reporting and information requirements of the Province, as contemplated under this Article 13 (*Reporting and Annual Operating Plan*), will not result in any increased Fees being payable by the Province. The Service Provider will at all times comply with the requirements of **Schedule 21** *(Reporting Requirements)*, as the same may be adjusted or amended from time to time, and will provide suggestions to the Province as to improvements, enhancements and changes to the reporting and informational requirements set forth in **Schedule 21** *(Reporting Requirements),* for Approval by the Province through the Governance Process.

13.4 Format of Reports.

To the greatest extent possible, the Parties will use web-enabled reports and direct electronic access to data and query reports to meet the reporting and informational needs of the Province. The Parties agree to minimize the amounts and types of paper based reporting.

13.5 Annual Operating Plan.

The Service Provider will, with the co-operation and assistance of the Province through the Governance Process, prepare and provide to the Province an annual operating plan (the **"Annual Operating Plan"**) that will be the planning document utilized in the provision of the Services, consisting of:

(a) a summary of the financial and operational changes for the Services in the next most immediate Contract Year, based upon the most current annual estimate available;

(b) a survey, review and analysis of the Systems and resources used to provide the Services;

(c) strategies to assist in realizing the objectives set forth in Section 1.13 (*Objectives of the Parties*);

(d) an analysis of the operations by the Service Provider with recommendations for changes to reduce costs, improve efficiencies and improve the satisfaction of the Clients of the Services, the Province and Stakeholders;

(e) a description of any planned changes to the Services for the following Contract Year, to the extent known;

(f) a description of any proposed material changes in the way the Service Provider wishes to provide the Services;

(g) a review and analysis of any projects performed over the previous Contract Year and summary of recommended projects for the next immediate Contract Year, to the extent known;

(h) any planned System or resource acquisitions (including changes to the number and type of Personnel currently providing the Services, whether by an increase or decrease in the number and FTE of such Personnel) to provide for additional or decreased Service capacity and volume, or to otherwise exploit new technological or business process developments;

(i) a description of the risk profile of the Service Provider, including a description of any material risks which could have an impact on the Service Provider's ability to provide the Services in accordance with Service Levels;

(j) a budget forecast setting out the estimated financial information in respect of the upcoming Contract Year, taking into account anticipated changes and information then available to the Service Provider (which budget will be consistent with the Economic Model, but subject to any changes having been made through the Change Order Process or otherwise); and

(k) such other matters as may be mutually agreed to by the Parties through the Governance Process.

13.6 Timing of Annual Operation Plan.

No later than 120 days prior to the commencement of the next Contract Year, the Service Provider will develop, prepare and provide to the Province, through the Governance Process, a proposed Annual Operating Plan for the next Contract Year, with the first Annual Operating Plan being delivered on or

before December 1, 2009. Within 30 days following receipt of the proposed Annual Operating Plan, the Parties, through the Governance Process, will jointly Approve the Annual Operating Plan or discuss any modifications or changes required thereto, and the Service Provider will provide the Province, through the Governance Process, with a revised Annual Operating Plan incorporating such modifications or changes. Any Dispute with respect to the Approval of the Annual Operating Plan will be resolved through the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*).

13.7 Annual Confirmation.

The Service Provider will deliver a certificate to the Province, together with the Annual Operating Plan referred to in Section 13.5 (*Annual Operating Plan*), that contains a confirmation signed by a senior officer or director of the Service Provider stating that:

(a) a review of the activities of the Service Provider during the preceding Contract Year has been made under the supervision of such senior officer or director; and

(b) based upon the review referred to in paragraph (a) above, and to the best of the knowledge of such senior officer or director, after having made due inquiry, the Service Provider has fulfilled all of its obligations under this Agreement in all material respects (including, without limitation, the Privacy Obligations), and that no Material Breach (or any event which, with notice or lapse of time or both, could reasonably be determined to become a Material Breach) occurred during such Contract Year in respect of such obligations, and stating exceptions to any of the forgoing, if applicable.

ARTICLE 14 – MAINTENANCE OF RECORDS

14.1 Maintenance of Records.

During the Term and for a period of seven (7) years after the end of the Term (or such longer period as may be required by Applicable Law, or in the case of Subcontractors who cease to provide Services, seven (7) years after such Subcontractors have ceased to provide Services), the Service Provider will:

(a) maintain accurate and complete Records related to this Agreement and to the Services to be provided by the Service Provider under this Agreement (other than Records which have been returned to the Province by the Service Provider), as may be required or necessary in order for the following, provided that the Service Provider will not be required to retain any specific Record for a period of greater than seven (7) years except as required by Applicable Law:

(i) the Service Provider to meet any other reporting or record keeping requirements referred to in this Agreement, and

(ii) to enable the Province to verify compliance by the Service Provider with the terms of this Agreement and to ascertain the accuracy of all financial matters arising under this Agreement; and

(b) cause Subcontractors to maintain complete and accurate Records of the transactions and activities undertaken by such Subcontractors as part of the Services (other than Records which have been returned to the Province by the Service Provider), as may be required or necessary in order for the following, provided that the Subcontractor will not be required to retain any specific Record for a period of greater than seven (7) years except as required by Applicable Law:

(i) the Service Provider to meet any other reporting or record keeping requirements referred to in this Agreement, and

(ii) to enable the Province to verify compliance by the Subcontractor with the terms of this Agreement and to ascertain the accuracy of all financial matters arising under this Agreement.

Without limiting the generality of the foregoing, the Service Provider will ensure that all New Records with respect to the performance of the Services will conform with GAAP (to the extent applicable), the requirements of Applicable Laws, and the Province's Administrative Records Classification System (ARCS) and Operational Records Classification Systems (ORCS), as may be amended from time to time and notified by the Province to the Service Provider, subject to the Change Order Process.

14.2 Transferred Records.

The Province will arrange for the delivery of the Transferred Records to the Service Provider on or before the Hand-Over Date, in accordance with the records protocols described in the attached **Schedule 22** *(Records Protocols)*.

14.3 Custody of Province Records.

The Service Provider will have Custody of the Province Records from the later of the date that Custody is granted to the Service Provider by the Province or the date of the creation or coming into existence of the Province Records, in accordance with and subject to the provisions of this Agreement.

14.4 Control of Province Records.

The Province Records will remain the property and in the Control of the Province, and accordingly, they will continue to remain subject to the requirements of the British Columbia *Document Disposal Act, Electronic Transactions Act, Freedom of Information and Protection of Privacy Act* (British Columbia) and all Province Policies related, thereto, and the *Interpretation Act*. The Service Provider will comply with the requirements thereof in respect of the Province Records as though each such Act or Policy applied to the Service Provider directly. In addition, the Service Provider will:

(a) not sell, transfer to the physical custody of another jurisdiction or Person, destroy or otherwise dispose of the Province Records without the Approval and direction of the Province, or as contemplated under this Agreement, and then, only in accordance with the protocols described in **Schedule 22** *(Records Protocols)*, and the provisions of Article 16 (*Privacy, Security and Confidentiality*);

(b) not under any circumstances, and without limiting the provisions of Article 16 (*Privacy, Security and Confidentiality*), use or disclose any Province Records except:

(i) on the prior written directions, or with the Approval, of the Province (which directions or Approval may be given by the Province at any time, in its sole discretion, or in response to a written request from the Service Provider specifying the particulars of the proposed use or disclosure of such Records), or

(ii) through the ordinary course provision of the Services as contemplated under the terms of this Agreement and in accordance with applicable Province Policies notified to the Service Provider from time to time;

(c) return the Province Records to the Province on the written instructions of the Province or as may otherwise be required or permitted in accordance with the provisions of this Agreement;

(d) at the request and expense of the Province, provide written or electronic copies of such Province Records for storage on the premises of the Province or of any applicable regulatory body or agency, as the Province may require;

(e) maintain the safe keeping and integrity of the Province Records in accordance with the records protocols set forth in the attached **Schedule 22** *(Records Protocols)* and with the provisions of Article 16 (*Privacy, Security and Confidentiality*);

(f) store all Province Records separately from other records of the Service Provider and identify them as Records of the Province; and

(g) provide the Province with copies of any Province Records, and permit the Province to have access to the Province Records with such access being in accordance with the provisions of Section 22.1 (*Access Rights*)).

The Province will comply with its obligations to the Service Provider in respect of the Province Records as set forth in **Schedule 22** *(Records Protocols).*

14.5 Final Return of Province Records.

Upon Termination of this Agreement, the Service Provider will deliver all such Province Records then in its Custody to the Province, including the performance of any obligations, steps or other requirements set forth in the Termination Assistance Plan. The Service Provider may, subject to the terms of Article 16 (*Privacy, Security and Confidentiality*), maintain sufficient copies of financial and other records following Termination of this Agreement, as it is required to maintain for tax and other statutory reasons in accordance with Applicable Laws.

14.6 Costs of Record Keeping.

The Service Provider acknowledges and agrees that all costs of record keeping contemplated in this Article 14 (*Maintenance of Records*) will be the responsibility of the Service Provider, and that compensation to the Service Provider in respect thereof is included in the Fees. For greater clarification, any Province Records delivered by the Service Provider to the Province at the request of the Province or pursuant to Sections 14.4 (*Control of Province Records*) and 14.5 (*Final Return of Province Records*), or **Schedule 22** *(Records Protocols)*, will thereafter be the responsibility (both financially and as to storage obligations) of the Province, unless such Province Records are returned to the Service Provider during the Term in accordance with the provisions of this Agreement.

14.7 Storage and Disposal of Records.

The Service Provider will transfer all Province Records identified by the Service Provider for storage, destruction or disposal to the Province in accordance with the record protocols more particularly described in **Schedule 22** *(Records Protocols)*, or as otherwise Approved by the Province. The Province will destroy any such Province Records if the Province determines it to be appropriate to do so. The Service Provider will not, without the Approval of the Province, dispose of or otherwise destroy any Province Records in its Custody at any time before the seventh (7^{th}) anniversary of the date that the final payment under this Agreement is made or of the date that all outstanding Disputes are settled, whichever is later.

14.8 Locations of Records.

Unless provided otherwise in this Agreement, and subject to the provisions of Section 5.1 *(Overview of Service Locations)*, the following provisions will apply in respect of all Province Records that contain any Personal Information:

(a) the Service Provider will maintain the Province Records in Canada at locations notified by the Service Provider to the Province in writing pursuant to Section 5.2 (*Service Locations*);

(b) the Service Provider will not relocate any such Province Records maintained pursuant to this Section without first notifying the Province in writing; and

(c) at no time will any Person have remote access to any Personal Information (including on any backup data) contained in the Province Records from any location outside of Canada, except as expressly Approved by the Province.

ARTICLE 15 – FEES AND PAYMENT TERMS

15.1 Fees.

In consideration of the performance of the Services, the Province will pay the Fees to the Service Provider, net of any amounts as contemplated pursuant to Article 8 *(Service Levels)*, or as otherwise contemplated in this Agreement. Except as otherwise expressly set forth in this Agreement, the Province will not be obligated to pay any other amounts to the Service Provider for the Service Provider's performance of the Services and its other obligations under this Agreement. Any expenses that the Service Provider incurs in the performance of the Services are included in the Fees, and accordingly, the Service Provider's expenses will not be separately reimbursable by the Province unless specifically provided otherwise under, or agreed pursuant to, the terms of this Agreement.

15.2 Invoices.

The Service Provider will provide the Province with monthly invoices, that conform to the payment requirements set forth in Section 15.3 (*Method of Payments*) and Schedule 23 (*Fees*), for all Fees that are payable from time to time by the Province pursuant to this Agreement. Each invoice will be provided in hardcopy form, and if requested by the Province in electronic form compatible with the Province's financial computer systems, and in either case with the level of detail as may be requested by the Province from time to time to satisfy the Province's internal accounting requirements. The payment of any invoice by the Province will not be deemed to be Approval or acceptance of such invoice, and no such payment will preclude the Province from contesting any amount set forth in an invoice at any later date in accordance with the provisions of Section 15.6 (*Disputed Payments*).

15.3 Method of Payment.

The Province will pay the Fees to the Service Provider on the following terms:

(a) the Fees will be payable monthly, in arrears, prior to the date which is sixty (60) days after receipt by the Province of an invoice from the Service Provider in a form that is in compliance with this Agreement, such invoice not to be delivered by the Service Provider to the Province before the end of the Service period for which it relates;

(b) notwithstanding the payment date set forth above, interest on any overdue amounts will only be payable at the rates and in respect of the periods as set forth in the *Interest on Overdue Accounts Payable Regulation* (B.C. Reg. 215/83), as amended or replaced from time to time, and where such regulation has been revoked and not replaced, at the last rate and time period calculated thereunder; and

(c) all Fees calculated or otherwise set forth in this Agreement are inclusive of all applicable Taxes unless otherwise expressly stated in this Agreement (including, without limitation, the provisions of Section 15.4 (*Taxes*)).

15.4 Taxes.

The Services contracted for under this Agreement are for the Province, are being paid for with Crown funds, and are therefore not subject to GST. The Service Provider will collect, remit to the appropriate Taxing Authorities and report to the Province on all Taxes related to the Services to the extent that the same are included in the Fees, and to the extent that any of the Services attract PST, the Service Provider will add the same to the invoices for the Fees. The Service Provider will be responsible for and will arrange to pay all other Taxes relating to the Services including Taxes based on its own capital, net income, employment taxes of its own employees and for taxes on any property it owns.

15.5 Right of Set-Off.

Any amounts owed to the Province:

(a) by the Service Provider under this Agreement or otherwise in respect of the Services, including Service Level Credits, but excluding any amounts under Dispute;

(b) by the Service Provider under any other agreement entered into now or in the future between the Service Provider and the Province that is not related to this Agreement, but excluding amounts in dispute thereunder in accordance with its terms; and

(c) by the Service Provider's Affiliates pursuant to the Corporate Guarantee;

may be set-off by the Province against Fees and other charges payable by the Province to the Service Provider under this Agreement, or may be deducted from any sum due or which at any time may become due to the Service Provider under this Agreement. To the extent that there are any amounts owing by the Service Provider to the Province upon the Termination of this Agreement, whether by credits or otherwise, and there are no further Fees to set-off such amounts, then the Service Provider will pay such amounts directly to the Province. The Province will give the Service Provider notice of such set-off under Section 15.5(b) above.

15.6 Disputed Payments.

Notwithstanding the payment of any Fees, the Province may dispute any amounts contained in an invoice within ninety (90) days of receipt of the invoice from the Service Provider. Notwithstanding the foregoing, if any overpayments by the Province should later be discovered as a result of an audit or investigation under Article 22 (*Audit Rights*) or otherwise, then the Province will be entitled to recover the amount of such overpayments by way of a Dispute, notwithstanding the fact that such overpayments are discovered after the expiry of such ninety (90) day period. In addition, the Province may withhold payment of a particular portion of Fees that the Province reasonably Disputes, subject to the following conditions:

(a) any amount so withheld will not exceed the amount alleged to be in error or not properly invoiced or payable, or for which no Services were performed;

(b) the Province provides to the Service Provider concurrently with the withholding of the disputed Fees, a detailed written explanation of the basis of the Dispute; and

(c) the Parties will promptly settle the Dispute regarding such amount in accordance with the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*).

Any interest accrued on any amount owed to or overpaid by the Province will be apportioned in the same manner as in the resolution of such disputed Fees. Any payment disputes will not affect the Service Provider's obligation to provide the Services under this Agreement at the agreed Service Levels or in accordance with any other of the Service Provider's obligations under this Agreement.

ARTICLE 16 – PRIVACY, SECURITY AND CONFIDENTIALITY

16.1 Privacy Obligations.

The Service Provider will at all times, and will ensure that its Personnel, and to the extent applicable in accordance with the provisions of **Schedule 24** *(Privacy Obligations)* its Subcontractors and External Personnel, comply with the obligations and requirements set forth in **Schedule 24** *(Privacy Obligations)*, as such are amended from time to time in accordance with this Agreement (the "**Privacy Obligations**").

16.2 Foreign Disclosures.

The Service Provider expressly acknowledges and agrees that it is subject to the laws of British Columbia and the laws of Canada applicable in British Columbia with respect to this Agreement and the performance of the Service Provider's obligations under this Agreement, and it is not subject to any Foreign Disclosure Laws including, without limitation, any orders, directives, rulings, requirements, judgments, injunctions, awards or decrees, decisions, or other requirements issued pursuant to any Foreign Disclosure Laws, or any directions or requests from any Affiliate of the Service Provider in respect of the same, and in each case, related to any Personal Information (each a "**Disclosure Order**"). The Service Provider will immediately inform the Province if the Service Provider receives a Disclosure Order. Upon receipt of a Disclosure Order, the Service Provider will not disclose any Personal Information in response thereto and the Service Provider will at all times act in accordance with the terms and conditions of this Agreement including, without limitation, the Privacy Obligations. Any breach of this Section will be a Material Breach under this Agreement. The provisions of this Section represent a lawful restriction on the Service Provider, being a Person governed by the laws of British Columbia and the laws of Canada applicable in British Columbia. The Service Provider will flow through the requirements of this Section to any Access Subcontractors, to apply to the Access Subcontractors, *mutatis mutandis*.

16.3 Corporate Structure and Corporate Chart.

As of the date of this Agreement, and as at the Hand-Over Date, the corporate organizational chart, indicating all shareholdings to the ultimate indirect shareholder (other than the shareholdings of a public company listed on a recognized stock exchange) of the Service Provider, the Performance Guarantor and the Corporate Guarantor (each a "**Corporate Structure**"), are as set forth in **Schedule 25** *(Corporate Chart)*. Throughout the Term, the Service Provider will provide the Province with an updated Corporate Structure from time to time forthwith upon any changes being made thereto; provided that the requirements of this provision will in no way provide the Service Provider with any relief from, or be deemed to be a waiver of, the provisions of Section 31.2 (*Assignment by Service Provider*). Unless

agreed otherwise by the Province, for so long as the Service Provider or the Performance Guarantor has, or could have, disclosure or use of, or access to any Personal Information in connection with the performance of the Services under this Agreement, or in connection with the application of the Performance Guarantee, as the case may be, the Service Provider and the Performance Guarantor will be and remain under the direct Corporate Control of a Canadian Entity, and any failure of the Service Provider or the Performance Guarantor to remain so controlled will be deemed to be a Material Breach under Section 28.1 (*Service Provider Material Breach*), and will give rise to the right of the Province to terminate this Agreement pursuant to Section 28.2 (*Remedies of the Province*).

16.4 Canadian Entities.

Throughout the Term, the Service Provider will ensure that the Access Subcontractors who are not individuals are corporations, partnerships, limited partnerships, or other similar entities that are incorporated or created under the laws of Canada or under the laws of any province of Canada (each a "**Canadian Entity**"), and that the Access Subcontractors who are individuals are not Foreign Employed Individuals. Unless agreed otherwise by the Province, and for so long as any Access Subcontractor has or could have any access to, or use or disclosure of, any Personal Information in connection with the performance of the Services under this Agreement, the Service Provider will ensure that:

(a) in the case of Access Subcontractors who are individuals, the Access Subcontractor are not, and do not become, a Foreign Employed Individual; and

(b) in all other cases, the Access Subcontractors are and remain a Canadian Entity, and unless otherwise Approved by the Province, a Canadian Entity that is Corporately Controlled by a Canadian Entity or by individuals who are not Foreign Employed Individuals.

16.5 Acknowledgement.

The Service Provider acknowledges that in the performance of the Services, the Service Provider will be given access to and Custody of highly confidential and sensitive information, including Province Confidential Information, and that the confidentiality, privacy and security of such information, and in particular the Personal Information, is of paramount importance to the Province.

16.6 Safeguarding Confidential Information.

Each of the Parties acknowledges and agrees that all Confidential Information of the other Party, whether received or created before or after the Hand-Over Date, will be received in the strictest confidence and will be held and used only in accordance with and subject to the terms of this Agreement. A Party receiving the Confidential Information of the other Party will retain such information in confidence and will treat such information in accordance with the terms of this Agreement (including the Privacy Obligations), and with a degree of care no less than the degree of care that the receiving Party employs for the protection of its own Confidential Information of a similar nature; provided that in any event the Service Provider will use a degree of care to protect such Confidential Information that is appropriate to the nature of the information and is in accordance with prudent industry practice for the data hosting and data centre facilities services in Canada. Without limiting the generality of the foregoing, and subject to the Change Order Process, the Service Provider further agrees to comply with such confidentiality, privacy and security Directives as issued by the Province from time to time.

16.7 Permitted Disclosure and Use of Confidential Information.

Subject to the Privacy Obligations and Section 16.2 (*Foreign Disclosures*), a Party may use or disclose relevant aspects of the other Party's Confidential Information:

(a) only to the extent necessary to perform its obligations and exercise its rights under this Agreement;

(b) only to its Personnel, Subcontractors, External Personnel and professional advisors (and in the case of the Province, its employees, contractors, professional advisors and agents) to the extent that such disclosure and use thereof is necessary for the performance of the receiving Party's rights or obligations under this Agreement, and provided that such Persons have an actual need to know such information and have signed non-disclosure agreements as required by this Agreement (to the extent applicable), it being agreed between the Parties that the provisions of this paragraph will in no way restrict or otherwise limit either Party from disclosing the Confidential Information of the other Party, to the extent necessary, to the receiving Party's legal advisors in the course of obtaining legal advice in connection with this Agreement, provided that the solicitor client privilege with respect thereto is not waived by the receiving Party in respect of such disclosure; and

(c) in the case of a disclosure of the Service Provider's Confidential Information by the Province, for purposes of undertaking any procurement or related process in connection with the selection of an Alternative Service Provider, provided that:

(i) such disclosure does not include any of the Service Provider's costing or other internal financial information,

(ii) any third parties to whom such disclosure is made first execute and deliver to the Province a Non-Disclosure Agreement and the Province provides such executed Non-Disclosure Agreement to the Service Provider, and

(iii) such disclosure will be restricted to the Service Provider Confidential Information necessary to enable such parties to participate in such procurement or related process.

16.8 Province Permitted Disclosure.

Notwithstanding the provisions of this Article 16 (*Privacy, Security and Confidentiality*), the Province may disclose the Service Provider Confidential Information as may be required by the provisions of any Applicable Laws, including the *Freedom of Information and Protection of Privacy Act* (British Columbia), as contemplated in Section 16.10 (*Disclosure Compelled by Law*) and as required by the Province in order to prevent any actual or reasonably anticipated disclosure of Personal Information. For purposes thereof, the Service Provider acknowledges that the Non-Disclosure Agreements referred to in Section 16.7 (*Permitted Disclosure and Use of Confidential Information*) will be subject to the requirements and obligations of that Act.

16.9 Exceptions to Obligation of Confidentiality.

Subject to the Privacy Obligations and Section 16.2 (*Foreign Disclosures*), the obligations of confidentiality contained in this Article 16 (*Privacy, Security and Confidentiality*) will not apply to any Confidential Information of the other Party to the extent that the receiving Party can reasonably demonstrate that such Confidential Information:

(a) was, at the time of disclosure to the receiving Party, in the public domain;

(b) after disclosure to the receiving Party, is published or otherwise becomes part of the public domain through no fault of the receiving Party, and where the receiving Party is the Service Provider, through no fault of the Service Provider's Affiliates or Subcontractors;

(c) was in the possession of the receiving Party at the time of disclosure to the receiving Party, and was not the subject of a pre-existing confidentiality obligation;

(d) was disclosed independently to the receiving Party by a third party who, insofar as the receiving Party was aware, was not subject to any confidentiality obligations in respect thereof, and in any event, provided that such information was not of a nature that had it been the Confidential Information of the receiving Party, the receiving Party would have required that it be kept confidential;

(e) was independently developed by the receiving Party without the use of any Confidential Information of the other Party;

(f) is disclosed with the prior Approval of the other Party, but only to the extent Approved by the other Party;

(g) is Service Provider Confidential Information and such information is required to be disclosed by the Province under the *Freedom of Information and Protection of Privacy Act* (British Columbia); or

(h) is Service Provider Confidential Information and such information is required to be disclosed by the Province in order to comply with Province Policies.

16.10 Disclosure Compelled by Law.

Subject to the Privacy Obligations and Section 16.2 (*Foreign Disclosures*), a Party will not be considered to have breached its confidentiality obligations under this Article 16 (*Privacy, Security and Confidentiality*) for disclosing any Confidential Information of the other Party to the extent that such disclosure is required to satisfy any Applicable Laws and, subject to Section 16.11 (*Disclosure of Personal Information*), expressly excludes Personal Information, provided that the Party required to make such disclosure (the "**Compelled Party**"):

(a) promptly upon receiving any such request and within a reasonable time prior to disclosure (if possible), notifies the other Party of the terms and circumstances of the requested disclosure;

(b) consults with the other Party regarding the nature and scope of such request and the response or other position that the Compelled Party intends to take with respect to such request;

(c) does not obstruct or interfere with, and to the extent practical, permits the other Party to obtain, a protective order or other remedy to prevent, object to, enjoin, narrow the scope of, or otherwise contest the requested disclosure;

(d) if the other Party is unable to obtain a protective order or other similar remedy within a time period that is appropriate in the circumstances, then the Compelled Party will only disclose such of the Confidential Information that it is legally obligated to disclose; and

(e) makes and reasonably pursues a request, that is reasonable and customary in the circumstances, to the applicable Governmental Authority, for confidential treatment of the information to be disclosed pursuant to such Applicable Laws.

16.11 Disclosure of Personal Information.

In respect of the Personal Information that constitutes Province Confidential Information, the Service Provider will not disclose to any Person or allow any Person to access or use, and will ensure that none of the Personnel, Subcontractors, or External Personnel disclose to any Person or allow any Person to access or use, the Personal Information, except:

(a) if, and in the manner expressly permitted pursuant to, the Privacy Obligations or to the provisions of the *Freedom of Information and Protection of Privacy Act* (British Columbia);

(b) as expressly Approved by the Province; or

(c) pursuant to an order of a Canadian court of competent jurisdiction in accordance with Section 16.12 (*Court Order Disclosure*).

16.12 Court Order Disclosure.

If the Service Provider is required, in order to satisfy any Applicable Laws, to disclose to any Person or to allow any Person to have access to any Personal Information other than as permitted in Subsections 16.11(a) to (b) (*Disclosure of Personal Information*), then the Service Provider will not disclose or allow access to the same unless and until the Service Provider:

(a) has provided the Province with written notice of such requirement;

(b) the Service Provider and the Province (at the Province's option) have appeared before a Canadian court having competent jurisdiction; and

(c) such Canadian court has ordered that the Service Provider disclose or allow access to the Personal Information.

16.13 Notification of Unauthorized Use of Confidential Information.

Each Party will:

(a) promptly notify the other Party of any unauthorized possession, use, access or disclosure of the other Party's Confidential Information by any Person, or attempt to effect the same, upon such information becoming known to such Party;

(b) promptly furnish the other Party with details of such unauthorized possession, use, access or disclosure, or attempt to effect the same, and assist the other Party in investigating or preventing the recurrence of any unauthorized possession, use, access or disclosure, or attempt to effect the same, of the other Party's Confidential Information;

(c) cooperate with the other Party in any litigation and investigation against third parties deemed necessary by the other Party to protect its Confidential Information, to the extent such litigation or investigation is related to this Agreement;

(d) reimburse the other Party for any direct expenses incurred by such other Party as a result of such other Party's compliance with paragraphs (a) – (c) above, unless such other Party has directly or indirectly caused or is otherwise responsible for any unauthorized possession, use, access or disclosure of the Party's Confidential Information, in which case such other Party will be solely responsible for any and all direct expenses incurred as a result of its compliance with this Section; and

(e) promptly use best efforts to prevent a recurrence of any unauthorized possession, use, access or disclosure of the other Party's Confidential Information, where such Party has directly or indirectly caused or is otherwise responsible for any unauthorized possession, use, access or disclosure of the other Party's Confidential Information by any Person.

16.14 Breach of Confidentiality.

In the event of a breach of this Article 16 (*Privacy, Security and Confidentiality*), and to the extent available pursuant to Applicable Laws (including, without limitation, the *Crown Proceeding Act* (British Columbia)), the non-defaulting Party will be entitled to preliminary and permanent injunctive relief, as well as an equitable accounting of all profits and benefits arising out of such breach, which remedy will be in addition to any other rights or remedies to which the Party may be entitled under this Agreement or otherwise under any Applicable Laws.

16.15 No Rights to Confidential Information.

Nothing contained in this Article 16 (*Privacy, Security and Confidentiality*) will be construed as obligating a Party to disclose its Confidential Information to the other Party, or as granting or conferring on a Party, expressly or implied, any right, title or interest or any licence in or to the Confidential Information of the other Party.

16.16 Ownership of Province Confidential Information.

The Province Confidential Information is and will remain the property of the Province. Subject to applicable security procedures and System availability, the Province will have complete and unrestricted Control and access at all times of and to the Province Confidential Information and, as part of the Services, the Service Provider will provide access thereto as may be requested by the Province from time to time, including such access as will enable the Province to make complete copies of all Province Confidential Information. Control of the Province Confidential Information is vested solely in the Province and nothing in this Agreement will in any way be construed to grant Control of the Province Confidential Information to the Service Provider or any other Person. The Service Provider will at all times adhere to the directions of the Province with respect to Province Confidential Information. On the Province's request, at any time during the Term or upon any Termination, the Service Provider will promptly return to the Province, in the format and on the media requested by the Province, all or any part of the Province Confidential Information, and erase or destroy all or any part of the Province Confidential Information in the Service Provider's or in any Service Provider Group member's possession, or in each case to the extent so requested by the Province.

ARTICLE 17 – BUSINESS CONTINUITY

17.1 General.

As part of the Services, the Service Provider will:

(a) on or before the Hand-Over Date, and as part of the Transition Services, review the Province's existing Business Continuity Plan for the Services and update such plan as may be reasonably determined necessary by the Service Provider, and subject to Subsection 17.2(a)(vii) for the Data Centre Services BCP, Approved by the Province;

(b) ensure that the Business Continuity Plan at all times expressly address all Force Majeure Events and Labour Disruptions;

(c) from and after the Hand-Over Date, assume all responsibility for the establishment and maintenance (including all related management, training, planning, plans, work products and deliverables) of the Business Continuity Plan for the Services, having regard to the roles and responsibilities of the Parties as set forth in Section 17.2 (*Roles and Responsibilities*);

(d) be responsible for all costs in respect of any updates to the Business Continuity Plan, unless specifically agreed otherwise by the Parties under the terms of this Agreement.

For greater clarification, the updated Business Continuity Plan Approved by the Province as contemplated in paragraph (a) above will be implemented and maintained by the Service Provider for the Term of this Agreement, subject to further amendments by the Service Provider in accordance with the terms of this Article 17 (*Business Continuity*), and will thereafter be, and be deemed to be, the Business Continuity Plan for purposes of this Agreement.

17.2 Roles and Responsibilities.

The roles and responsibilities of the Parties in respect of the Business Continuity Plan and the Disaster Recovery Plan for the Services will be as set forth in this Article 17 (*Business Continuity and Disaster Recovery*) including, without limitation, the following:

(a) the roles and responsibilities of the Province are as follows:

(i) to lead the Ministry's business continuity planning,

(ii) to provide standards and templates to the Service Provider if and to the extent that the Province requires that the Service Provider use or follow the same,

(iii) at the request of the Service Provider, to provide clarification regarding the interpretation or application of applicable Province Policy,

(iv) subject to Subsection 17.2(a)(viii) for the Data Centre Services BCP, at the option of the Province, to participate in and review any test activities of the Business Continuity Plan for the Services,

(v) to review the Business Continuity Plan for the Services from time to time to ensure that they comply with and otherwise conform to applicable Province Policy (including any applicable Ministry policy) and the requirements of this Agreement, and to the extent that the Province determines, in its sole discretion, that the Business Continuity Plan does not so comply, then upon receipt of written notice thereof from the Province the Service Provider will forthwith update and amend the Business Continuity Plan to the extent required for the Business Continuity Plan to be fully compliant with the applicable Province

Policy (including any applicable Ministry policy) and the requirements of this Agreement,

(vi) to communicate with Clients and Stakeholders regarding the integration and co-ordination of the Service Provider's Business Continuity Plan for the Services with those of the Stakeholders,

(vii) to establish applicable Recovery Time Objectives in respect of the Business Continuity Plan for the Services, in consultation with the Service Provider through the Governance Process, and

(viii) at the invitation of the Service Provider, the Province will participate in and review any test activities of the Data Centre Services BCP; and

(b) the roles and responsibilities of the Service Provider are as follows:

(i) to comply with applicable Province Policy (and any applicable Ministry policy), and the terms of this Agreement, relating to business continuity and disaster recovery, and upon receipt of a written notice from the Province that the Business Continuity Plan does not so comply with the same, to forthwith update and amend the Business Continuity Plan to the extent required for the Business Continuity Plan to be fully compliant with the applicable Province Policy (including any applicable Ministry policy) and the requirements of this Agreement,

(ii) to provide business continuity and disaster recovery services to the Province and to take responsibility for the Business Continuity Plan in respect of the Services, in accordance with the provisions of this Article 17 (*Business Continuity*),

(iii) to ensure that its Subcontractors are able to meet the requirements of the Business Continuity Plan for the Services to the extent applicable to them, and with respect to the Data Centre Services BCP, annually obtain and provide to the Province a certificate from the applicable Subcontractor that the Data Centre Services BCP is fully compliant with applicable Province Policy (and any applicable Ministry Policy) and the terms of this Agreement relating to business continuity and disaster recovery for the Data Centre Services,

(iv) to provide the Province with information and cooperation (and participation) in respect of the Business Continuity Plan for the Services as may be requested by the Province from time to time,

(v) to notify the Province (through the Province Business Continuity Representative) in the event of the declaration of a Disaster and the resulting requirement to activate a Business Continuity Plan for the Services, and

(vi) to ensure the effectiveness, preparedness and ability of the Service Provider to execute the Business Continuity Plan for the Services.

17.3 Service Provider Representative.

The Service Provider will designate a "Business Continuity Representative", who may be identified as a Key Position, to be responsible for:

(a) the upkeep, testing and implementation of the Business Continuity Plan for the Services; and

(b) acting as the liaison with the Province to ensure the integration of the Service Provider's Business Continuity Plan for the Services with those of the Province and Stakeholders (to the extent applicable).

The Service Provider will also designate an alternate representative (or representatives), who need not be a Key Position, to act as the "Business Continuity Representative" if the original designated representative is unavailable for any reason.

17.4 Plan Management and Annual Reviews.

From and after the Hand-Over Date, the Service Provider will be responsible for managing the continuity of the Services, in accordance with the business continuity and disaster recovery Province Policies, and pursuant to the Business Continuity Plan for the Services. The management of the Business Continuity Plan will include, without limitation, the following:

(a) the performance in each Contract Year of business impact assessments in respect of the Services;

(b) the performance in each Contract Year of strategic risk assessments in respect of the Services;

(c) the development of risk mitigation and business continuity and disaster recovery treatments in respect of the Services;

(d) to the extent applicable, the development of a Business Continuity Plan specifically for any essential Services as may be so notified by the Province to the Service Provider from time to time; and

(e) a review and update of the Business Continuity Plan for the Services at least once per Contract Year.

Any changes to the Business Continuity Plan for the Services may be submitted by either Party to the other in accordance with the Governance Process, or through the Change Order Process, as applicable. For greater clarification, the Province will have the right to review any changes to the Business Continuity Plan for the Services to ensure compliance with Province Policy (and any applicable Ministry policy), and the terms of this Agreement, prior to implementation thereof.

17.5 Recovery Time Objectives.

The Recovery Time Objectives for the Services will be reviewed, confirmed and Approved by the Parties through the Governance Process within six (6) months after the Hand-Over Date. Thereafter, and in each Contract Year, the Parties will review the Recovery Time Objectives, and will mutually agree on any revisions to the Recovery Time Objectives through the Governance Process, or will otherwise amend the Recovery Time Objectives through the Change Order Process, as applicable.

17.6 Testing of Business Continuity Plan.

The testing of the Business Continuity Plan for the Services will be performed by the Service Provider in accordance with applicable Province Policy in respect thereof. The testing will consist of process

walkthrough and awareness testing (as opposed to full production testing), except as specifically provided otherwise below. Such testing will include the following (to the extent consistent with the foregoing and as may applicable to the Service Provider):

(a) the Service Provider will complete a test of the Business Continuity Plan for the Services within such period following the Hand-Over Date as is specified in **Schedule 5** (*Special Terms*);

(b) the Service Provider will test the Business Continuity Plan for the Services with such frequency following the initial test described in paragraph (a) above as is specified in **Schedule 5** (*Special Terms*);

(c) the testing will include fail-over testing from the Service Provider's production facility to its back-up site;

(d) the Service Provider may carry out the fail-over tests at such times and in such manner (including a single complete test or successive partial tests) as the Service Provider deems appropriate;

(e) the Service Provider will conduct the testing in a manner that causes minimal disruption to the ongoing operations of the Services, and in full consultation with the Province;

(f) the Service Provider will complete a test of the Business Continuity Plan for the Services within such period as is specified in **Schedule 5** (*Special Terms*) of implementing any material change in respect of the Services (including, without limitation, any material change in the technology, processes, facilities, infrastructure, Systems or Recovery Time Objectives), for purposes of determining the impact of such material changes to the Services and the effectiveness of the Business Continuity Plan in respect thereof;

(g) subject to Subsection 17.2(a)(viii) for the Data Centre Services BCP, the Province will have the right to participate in any testing of the Business Continuity Plan for the Services as an observer in the testing process and to review any results of such testing;

(h) within thirty (30) days of any testing conducted by the Service Provider in respect of the Business Continuity Plan for the Services, the Service Provider will prepare and submit to the Province, through the Governance Process, a report detailing the results of such testing and listing any deficiencies in respect thereof, together with the Service Provider's proposed action plan and assigned responsibilities and timelines that will be undertaken by the Service Provider to address such deficiencies, and the Service provide will forthwith take all such steps and to all such things as may be necessary to carry-out and implement such action plan.

17.7 Actual Disaster.

In the event of a Disaster, or either Party's anticipation of a Disaster, the following provisions will apply:

(a) if the Service Provider is prevented from, or delayed in, performing any of its obligations under this Agreement as a result of the Disaster, or anticipates that it will be so prevented or delayed, then the Service Provider will promptly notify the Province thereof, and will provide the Province with a follow-up written notice within two (2) Business Days of the Service Provider becoming aware of the potential disruption, non-performance or delay, the particulars thereof including details of the nature of the event causing the same, its

expected duration and the obligations under this Agreement that will be affected as a result;

(b) the Service Provider will continue to provide detailed reports to the Province with respect to such disruption, non-performance or delay, on a timely basis during the continuance thereof;

(c) the Service Provider will restore all Services in accordance with the Business Continuity Plan for the Services (including the redeployment or reassignment of other available personnel to assist with the implementation of the Business Continuity Plan), having regard to the nature and extent of the Disaster and its impact on the Services, the Province, the Stakeholders and Clients of the Services;

(d) to the extent that the Disaster is not addressed or not fully addressed in the Business Continuity Plan for the Services, the Service Provider will use its best efforts to restore the Services;

(e) within thirty (30) days of the recovery of the Services as a result of the implementation of the Business Continuity Plan for the Services, the Service Provider will provide the Province with a written report detailing the root cause of the disruption, the steps taken by the Service Provider in respect thereof, and any recommendations that the Service Provider may have with respect to improving the Business Continuity Plan for the Services (including the responsibilities and timelines referred to therein);

(f) subject to the provisions of Article 30 (*Force Majeure and Labour Disruption*), if contrary to the Recovery Time Objectives, or as a result of the negligence of the Service Provider, the Service Provider does not materially restore the Services in accordance with the Business Continuity Plan for the Services, then the Province will be entitled to procure such services from another service provider (to the extent possible), and may off-set the costs thereof against the Fees payable to the Service Provider;

(g) notwithstanding the foregoing, the Province will retain the right to audit, sign-off and confirm the full recovery of the delivery of the Services following the implementation of the Business Continuity Plan for the Services; and

(h) there will be no Service Level Credits assessed or otherwise applied by the Province against the Service Provider during the continuance of a Disaster that is beyond the reasonable control of the Service Provider until full recovery of the delivery of the Services pursuant to the Business Continuity Plan, provided that the Service Provider complies, in all material respects, with its obligations under the provisions of this Article 17 (*Business Continuity*).

ARTICLE 18 – TECHNOLOGY, ARCHITECTURE AND IMPROVEMENTS

18.1 Architecture Standards.

In addition to the obligations otherwise set forth in this Agreement, the Service Provider will implement the Province's existing technical architecture standards and guidelines to the same extent as such standards and guidelines are themselves complied with by the Province as of the Hand-Over Date, as such standards are updated or revised by the Province from time to time (subject to the Change Order Process). The Service Provider will advise the Province of any significant incompatibilities known to the Service Provider that would result from changes to such standards. If

the Province requests the Service Provider's assistance to document technical architecture standards, then the Service Provider will deliver a draft manual setting out the technical architecture standards within three (3) months of the request. The Service Provider will update the Manual from time to time during the term as such standards change (and in accordance with the Change Order Process). The architectural standards and guidelines will form part of the Manual.

18.2 Technology Improvements and Currency.

The Service Provider will provide the Services by maintaining the supporting technologies at an appropriate level of currency and in a manner that will support the Parties' efforts to achieve the objectives set forth in Section 1.13 (*Objectives of the Parties*), and to comply with the Service Levels and the Privacy Obligations. Except as specifically, provided otherwise in this Agreement, the Service Provider will determine the appropriate levels of technology currency, and throughout the Term will identify and implement technology improvements, all with the Approval of the Province, and in accordance with the applicable provisions of **Schedule 5** (*Special Terms*). Except where the Province agrees in writing that such implementations are not necessary, the Service Provider will report to the Province at the end of each Contract Year throughout the Term, demonstrating its actions or steps that the Service Provider has taken to meet its obligations relating to improvements in technology set forth in this Section 18.2 (*Technology Improvements and Currency*).

18.3 Material Technology Change.

Before making any changes to the material suppliers of technology to be used by the Service Provider in performing the Services, the Service Provider will consult with the Province in respect thereof through the Governance Process, and will obtain the Approval of the Province to any such change, unless the requirement to obtain such Approval is waived in writing by the Province on a case by case basis.

18.4 Technology Presentations.

At the Province's request and cost, the Service Provider will facilitate the attendance of the Province personnel at any presentation offered to the Service Provider by any technology vendor whose software, equipment or materials are used, or are being considered by the Service Provider for use, directly or indirectly in a material manner in the provision of Services, except in the event that the Service Provider cannot obtain the consent of such technology vendor.

18.5 System Contaminants.

The Service Provider will ensure that all Systems provided or used by it, or by its Subcontractors or Suppliers, to provide the Services do not and will not contain any virus, Trojan horse, worm, backdoor, shutdown mechanism or similar software, code or program which is intended to, is likely to or has the effect of disabling, denying authorized access to, damaging or destroying, corrupting or affecting the provision of the Services or the normal use of any of the Service Provider's or the Province's Systems, networks or software, or any data on or used in conjunction therewith (each a **"Contaminant"**). The Service Provider will not insert, or knowingly permit any third party to insert, a Contaminant into any of the Systems used to provide the Services. In the event the Service Provider becomes aware of the existence of a Contaminant, it will notify the Province thereof and will remove the Contaminant in a prompt and co-ordinated manner so as to minimise the spread and impact of such Contaminant.

18.6 System Protection Features.

To the extent that any Software (either Service Provider Developed Software or Service Provider Licensed Software), including any Modifications thereto, that is, or at anytime hereafter may be, utilized

in providing Services under this Agreement contains protection features designed to prevent copying or the use of such Software or other unauthorized access, to disable or erase Software or data, to shut down all or any portion of the Services or to perform other like actions, the Service Provider will, in the case of:

(a) Service Provider Developed Software, provide the Province with the necessary key, password or other means for the Province to have continued access and use of such Software, in accordance with the provisions of Article 22 (*Intellectual Property*); and

(b) Service Provider Licensed Software, provide the Province with the necessary key, password or other means for the Province to have continued access and use of such Software, subject to license terms negotiated by the Service Provider, provided that the Service Provider will use commercially reasonable efforts to obtain any third party rights necessary to give effect to the foregoing and where the Service Provider is not able to obtain such third party rights, then Service Provider will inform the Province, in writing, and the Province shall have the right to Approve the use of such Software.

ARTICLE 19 – INTELLECTUAL PROPERTY AND PROPRIETARY RIGHTS

19.1 Ownership of Province Assets.

Except as expressly provided in this Agreement, the Province will be and remain the exclusive owner of all rights, title and interest in and to all assets and property provided by the Province to the Service Provider, including any assets to which the Service Provider is given access to by the Province from time to time during the Term.

19.2 Ownership of Province Proprietary Software.

The Province will be and remain the sole and exclusive owner of all rights, title and interest, including all Intellectual Property Rights, in and to:

(a) all Province Proprietary Software; and

(b) all Modifications of the Province Proprietary Software, whether made by or on behalf of the Province or the Service Provider, separately, jointly or with any other Person (including any of the Service Provider, Subcontractors, Personnel or External Personnel), and including where any Province Proprietary Software or any Modification thereto has been incorporated into any of the SP Proprietary Software.

Except as expressly provided otherwise under this Agreement, nothing in this Agreement or in the relationship between the Parties will confer any right or license in or upon the Service Provider in respect of the Province Confidential Information.

19.3 Ownership of SP Proprietary Software.

The Service Provider will be and remain the sole and exclusive owner of all rights, title and interest, including all Intellectual Property Rights, in and to:

(a) all SP Proprietary Software; and

(b) all Modifications to the SP Proprietary Software that are used in connection with the Services provided under this Agreement, whether made by or on behalf of the Service Provider (or its Subcontractors or its or their Affiliates, as the case may be) or the

Province, separately or jointly or with any other Person, and including where any Modifications have been incorporated into any of the SP Proprietary Software.

Except as expressly provided otherwise under this Agreement, nothing in this Agreement or in the relationship between the Parties will confer any right or license in or upon the Province in respect of the Service Provider Confidential Information.

19.4 Ownership of Third Party Software.

The parties acknowledge that with respect to any Third Party Software, the relevant third party Person who is the licensor of such Third Party Software will be deemed to be the sole and exclusive owner of all rights, title and interest, including all Intellectual Property Rights, in and to such Third Party Software.

19.5 Assignment of Intellectual Property.

If, notwithstanding Section 19.2 (*Ownership of Province Proprietary Software*) and Section 19.3 (*Ownership of SP Proprietary Software*), either Party (the "**Assigning Party**") retains, acquires or owns any right, title or interest, including any Intellectual Property Rights, in or to any Intellectual Property Rights, in or to anything that is to be owned by the other Party (the "**Assignee Party**") pursuant to Section 19.2 (*Ownership of Province Proprietary Software*) and Section 19.3 (*Ownership of SP Proprietary Software*), as applicable, (the "**Assigned Intellectual Property**"), then the following provisions will apply:

(a) the Assigning Party will assign, and for no further consideration and without any further act or formality does hereby irrevocably assign, to the Assignee Party all of the Assigning Party's worldwide right, title and interest in and to any Assigned Intellectual Property and any Modifications thereto, including all Intellectual Property Rights therein, free and clear of all Liens, but subject to the provisions of Section 19.8 (*License to Use Province Proprietary Software for the Services*) and Section 19.11 (*Use of SP Licensed Software*);

(b) if and to the extent that the assignment pursuant to this Section is not effective on the date hereof or on any future date, either generally or pursuant to any Applicable Laws, then any and all right, title and interest, including the Intellectual Property Rights, in and to any Assigned Intellectual Property or Modifications thereto that is retained, acquired or owned by the Assigning Party (collectively, the "**Assignee Trust Rights**"), will be held by the Assigning Party in trust for the exclusive benefit and use of the Assignee Party and its designates, except for the rights granted to the Service Provider pursuant to Sections 19.8 (*License to Use Province Proprietary Software for the Services*) and Section 19.11 (*Use of SP Licensed Software*); and

(c) the Assigning Party will execute and deliver to the Assignee Party such reasonable transfers, assignments, documents and instruments (promptly upon receipt thereof from the Assignee Party) as may be necessary to transfer and assign to the Assignee Party the Assignee Trust Rights, free and clear of all Liens, and will otherwise cooperate with the Assignee Party to give effect to, record and register the Assignee Party's ownership of the Assignee Trust Rights.

19.6 Service Provider Personnel, Subcontractors and External Personnel.

The Service Provider will ensure that all Personnel, Subcontractors and External Personnel will:

(a) by duly executed written agreement or by operation of law, irrevocably and unconditionally sell, assign and transfer to the Service Provider all right, title and interest, including all Intellectual Property Rights, that they may have in or to any or all Province Proprietary Software and all Modifications thereto, such that the assignment by the Service Provider pursuant to Section 19.5 (*Assignment of Intellectual Property*) includes any such right, title and interest, including all Intellectual Property Rights, of the Personnel, Subcontractors and External Personnel; and

(b) by duly executed written agreement or waiver document, irrevocably waive all non-transferable rights, including moral rights that they have or may have in any Province Proprietary Software or any Modifications thereto, in favour of the Service Provider, the Province and their respective successors and assigns.

If requested by the Province, and without limiting the Service Provider's obligations pursuant to this Section, the Service Provider will itself execute, and will obtain the execution by all Personnel, Subcontractors and External Personnel of all reasonable formal assignment documents requested and prepared by the Province, and the execution of all lawful oaths and applications for registration of the same in Canada, at Service Provider's cost, and in foreign countries, at the Province's cost.

19.7 Province Personnel and Contractors.

(a) The Province shall do such things as necessary to ensure that the Province acquires from any Province employees and contractors such right, title and interest, including Intellectual Property Rights, as may be necessary for the Province to assign to Service Provider all right, title and interest, including all Intellectual Property Rights, in and to the SP Proprietary Software and any Modifications thereto in accordance with Section 19.3 (*Ownership of SP Proprietary Software*) and Section 19.5 (*Assignment of Intellectual Property*).

(b) If requested by Service Provider, the Province shall use reasonable efforts to obtain from any Province contractors and employees of Province contractors written waivers of moral rights in respect of any Intellectual Property created or contributed to by such Province contractors and employees of Province contractors pursuant to this Agreement and which form part of the SP Proprietary Software or any Modifications thereto.

19.8 License to Use Province Proprietary Software for the Services.

Subject to the provisions of this Agreement, the Province hereby grants to the Service Provider the non-exclusive right during the Term, without cost or charge but subject to any third party rights as notified by the Province to the Service Provider, to use and copy the Province Proprietary Software and create and use any Modifications thereto, for the purpose of providing the Services pursuant to, and in accordance with, the terms of this Agreement, but subject to any restrictions, license terms or policies as reasonably determined by the Province, and any third party rights therein, all as may be notified in writing by the Province to the Service Provider. In connection therewith, the following provisions will apply:

(a) the Province will provide the Service Provider with any necessary third party rights to give effect to the foregoing rights granted to the Service Provider;

(b) the foregoing rights granted to the Service Provider do not give the Service Provider the right, and the Service Provider is not authorized, to market the Province Proprietary Software or Modifications thereto or to authorize any other Person to use the Province Proprietary Software or Modifications thereto (other than the Service Provider's

Subcontractors who require the same for purposes of, and in connection with, the delivery of the Services to the Province);

(c) the Province may authorize or license any third parties to use the Province Proprietary Software and any Modifications thereto during the Term, it being acknowledged that to the extent that such authorization or license may have an impact on the Services or on the Service Provider's rights and obligations relating to the Services, or require the Service Provider to provide additional services whether to the Province or any other Person, then the impact will be dealt with pursuant to the Change Order Process;

(d) the Service Provider is not permitted to use the Province Proprietary Software or any Modifications thereto for the benefit of any other Person without the prior written consent of the Province, provided that the Service Provider will have the right to authorize its Subcontractors to use the Province Proprietary Software and any Modifications thereto for the purpose of providing the Services pursuant to, and in accordance with, the terms of this Agreement;

(e) the foregoing rights are granted on an "as is" basis without warranties or conditions of any kind, whether oral or written or express or implied, and the Province specifically disclaims any implied warranties or conditions of merchantability, satisfactory quality, non-infringement and fitness for a particular purpose; notwithstanding the foregoing, this Subsection 19.8(e) shall not derogate from the indemnities provided in **Schedule 30** (*Indemnification Matters*)

(f) the foregoing rights will terminate upon the Termination Date or the expiry of the Termination Assistance Period, which ever is the later (the **"License Termination Date"**), subject to specific rights required with respect to the Termination Assistance Services; and

(g) if the Parties agree to integrate any Province Proprietary Software or Modifications thereto with any SP Proprietary Software, then prior to the integration thereof, the Parties shall enter into a written agreement setting out the Service Provider's rights to use such Province Proprietary Software and Modifications thereto after the Term, and any benefits that may be granted to the Province in connection therewith.

For the purposes of clarity, the license granted in this Section 19.8 shall be deemed to be in effect for any Province Proprietary Software as of the date on which the Service Provider provides the relevant Services utilizing such Province Proprietary Software or as the Parties may otherwise agree in writing.

19.9 Use of Province Licensed Software.

During the Term, and subject to the other terms of this Section, the Province will:

(a) at its own expense, obtain a right for the Service Provider and its Subcontractors to use the Province Licensed Software, as applicable, and only to the extent required to perform the Services;

(b) at its own expense, pay all fees for maintenance and support currently subscribed for by the Province for the Province Licensed Software used or accessed by the Service Provider and its Subcontractors,

(c) not assign or otherwise dispose of the licenses relating to the Province Licensed Software or amend, or terminate the licenses and the maintenance and support arrangements for the Province Licensed Software, in all cases, in any way which would materially adversely impact the Service Provider's ability to deliver the Services; and

(d) exercise all rights of renewal under its maintenance and support arrangements in relation to the Province Licensed Software during the Term such that during such time as the Service Provider is utilizing any Province Licensed Software in connection with the Services, the Province maintains maintenance and support arrangements for such Province Licensed Software as are appropriate to the performance of the Service Provider's obligations under this Agreement..

Notwithstanding the foregoing, under no circumstances will the Service Provider use, or be permitted to use, any or all of the Province Licensed Software for any purpose whatsoever other than to provide the Services under the terms of this Agreement. For any Province Licensed Software, the provisions of this Section 19.9 shall be in effect for such Province Licensed Software on or prior to the date on which the Service Provider provides the relevant Services utilizing such Province Licensed Software.

19.10 License to Use SP Proprietary Software.

Subject to the terms of this Agreement including, without limitation, Section 19.15 *(SP Proprietary Software–License to Province after Term and Related Matters)*, the Service Provider hereby grants to the Province the non-exclusive right during the Term, without cost or charge to use the SP Proprietary Software including, without limitation, any SP Affiliate Bespoke Software, and any Modifications thereto to the extent necessary for the Province to receive and enjoy the benefits of the Services or to perform its obligations under this Agreement. The Service Provider will provide to the Province any third party rights necessary to give effect to the foregoing. For the purposes of clarity, the license granted in this Section 19.10 (*License to Use SP Proprietary Software*) shall be deemed to be in effect for any SP Proprietary Software as of the date on which the Province receives and enjoys the benefits of the relevant Services utilizing such SP Proprietary Software or as the Parties may otherwise agree in writing.

19.11 Use of SP Licensed Software.

Subject to the terms of this Agreement including, without limitation, Section 19.12 (*Assignment of SP Licensed* Software) and Section 19.13 (*Third Party Software*), during the Term the Service Provider will:

(a) ensure that the Province has the non-exclusive right during the Term, without cost or charge except as provided in **Schedule 30** (*Fees*) or **Schedule 43** (*Software Responsibility Table*), but subject to any restrictions agreed to by the Province in respect of any Third Party Software, to use the SP Licensed Software to the extent necessary for the Province to receive and enjoy the benefits of the Services or to perform its obligations under this Agreement;

(b) at its own expense, pay all fees for maintenance and support for the SP Licensed Software used or accessed by the Province,

(c) not assign or otherwise dispose of the licenses relating to the SP Licensed Software or amend, or terminate the licenses and the maintenance and support arrangements for the SP Licensed Software, in all cases, in any way which would materially adversely impact the Province's ability to receive and enjoy the benefits of the Services; and

(d) exercise all rights of renewal under its maintenance and support arrangements in relation to the SP Licensed Software such that during such time as the Service Provider is utilizing any SP Licensed Software in connection with the Services, the Service Provider maintains maintenance and support arrangements for such SP Licensed Software as are appropriate to the performance of its obligations under this Agreement.

Notwithstanding the foregoing, under no circumstances will the Province use, or be permitted to use, any or all of the SP Licensed Software for any purpose whatsoever other than to receive and enjoy the benefits of the Services under the terms of this Agreement.

19.12 Assignment of SP Licensed Software.

During the Term, in respect of any license with:

(a) a third party Person for Third Party Software, except for the SP Leveraged Software, or

(b) an Affiliate of the Service Provider who is the licensor of any SP Affiliate Commercial Software,

the Service Provider will obtain as a provision of such license and at the time of obtaining such license (or prior to the use of such Third Party Software in providing the Services), the right to assign the license to the Province or an Alternative Service Provider without consent from, or a license transfer fee or other similar fee payable to such third party Person or Affiliate of the Service Provider, as the case may be, (and for greater clarification, excluding ordinary course ongoing license fees and maintenance costs in respect of such Third Party Software); provided that where the inclusion of such provision increases the cost of obtaining such license, then the Service Provider will be relieved of its obligation to obtain such right if it: (i) informs the Province of such increased cost (and provides the Province with detailed back-up documentation in support thereof), and (ii) provides the Province with an alternate replacement Software that is fully-assignable to the Province and provides the same functionality and performance as such Third Party Software (the "**Alternate Licensed Software**"), along with detailed information and back-up on all applicable license fees and other material costs associated with the Service Provider's use of such Alternate Licensed Software.

In addition, upon the earlier of 18 months prior to the License Termination Date or immediately upon the earlier termination of this Agreement, the Service Provider shall provide to the Province a full inventory of all SP Licensed Software being used by the Service Provider in providing Services at such time and confirm which such Third Party Software is: (xx) assignable to the Province without consent and at no cost, and (yy) assignable to the Province upon consent or payment of a license transfer or other similar fee to the relevant third party Person, and the Alternate Licensed Software (including all license fees and material costs associated therewith) to such Third Party Software.

19.13 Third Party Software.

The Service Provider will not incorporate, embed, contain or otherwise include in any Province Intellectual Property, Province Proprietary Software, Province Licensed Software or Modifications thereto any SP Proprietary Software, Third Party Software or any other Intellectual Property that is not Province Intellectual Property unless, subject to Section 19.11 (*Use of SP Licensed Software*), Service Provider has granted or obtained and assigned to the Province a license in respect of such SP Proprietary Software, Third Party Software or Intellectual Property on such terms and conditions as have been approved by the Province, in its discretion, prior to such provision, delivery, incorporation, embedding, containing or inclusion of that SP Proprietary Software, Third Party Software or any other Intellectual Property.

19.14 Intellectual Property Rights Re: New Services.

The Province and the Service Provider acknowledge that it is their intention to expand the scope of the Services in accordance with this Agreement, and recognize that, in connection with any new services, it will be necessary to reach an agreement on their respective Intellectual Property Rights in the Software that is then operated by the Province or other third parties. It is the intention of the Parties to resolve any issues associated with such Intellectual Property Rights on a basis that is consistent with the provisions of this Article 19 (*Intellectual Property and Propriety Rights*).

19.15 SP Proprietary Software – License to Province after Term and Related Matters.

Upon the expiry or termination of this Agreement, the Service Provider shall grant to the Province an irrevocable, non-exclusive, royalty-free, fully-paid up license and right to use the SP Proprietary Software to continue enjoying services that are comparable to the Services hereunder (including providing the Province with the same functionality in its Systems during the Term) for a period ending the earlier of the date that: (i) is one year after the License Termination Date, or (ii) an Alternative Service Provider starts to provide the Services; thereafter the license granted to the Province under this Section 19.15 is subject to the following:

(a) For any SP Proprietary Software including, without limitation, any SP Affiliate Bespoke Software, for which the Province and the Service Provider or the relevant SP Affiliate, as the case may be, have entered into a separate license agreement ("**Documented SP Software**") the Province shall continue to use such Documented SP Software in accordance with the terms of the relevant license agreement, which shall include at least the equivalent use rights as those set forth in Section 19.10 (*License to Use SP Proprietary Software*) (upon payment of the applicable license fees as provided for in the applicable license agreement);

(b) For any SP Proprietary Software including, without limitation, any SP Affiliate Bespoke Software, for which the Province and the Service Provider or the relevant SP Affiliate, as the case may be, have not entered into a separate license agreement ("**Undocumented SP Software**"), then the Service Provider or the relevant SP Affiliate, as the case may be, will offer to the Province at least one of the following options:

(i) a license to use the Undocumented SP Software on the terms set out in Section 19.10 (*License to Use SP Proprietary Software*) and this Section 19.15 (upon payment of the applicable license fees as provided for in this Agreement), which the Province may, in its discretion, accept (in which case the Province's right to use the Undocumented SP Software will be governed by that license agreement) or reject;

(ii) replacement Software that provides the same functionality and performance as the Undocumented SP Software and which will operate within the Systems without any degradation thereof or adverse effect thereon and which the Province may use in accordance with Section 19.10 (*License to Use SP Proprietary Software*) (upon payment of license fees that are at the normal commercial rates for the relevant replacement Software), (the "**Replacement SP Software**"), in which case the Province will continue to use the Undocumented SP Software in accordance with Section 19.10 (*License to Use SP Proprietary Software*) and this Section 19.15 until the Province has accepted the Replacement SP Software in accordance with the procedures for Acceptance Testing, at which time the

Province will return the Undocumented SP Software to the Service Provider and cease to have any right to use the Undocumented SP Software; or

(iii) the Service Provider or the relevant SP Affiliate, as the case may be, may allow the Province to continue to use the Undocumented SP Software in accordance with Section 19.10 (*License to Use SP Proprietary Software*), in which case the Service Provider will deliver, or procure the delivery of, to the Province the Source Materials in accordance with Subsection 19.15(e);

and if the Service Provider or the relevant SP Affiliate, as the case may be, does not provide the Province with at least one option under this Subsection 19.15(b) within 60 days after the end of the License Termination Date the Service Provider or the relevant SP Affiliate, as the case may be, will be deemed to have elected to proceed under Subsection 19.15(b)(iii);

(c) The Province will continue to have the right to use the Undocumented SP Software in accordance with Section 19.10 (*License to Use SP Proprietary Software*) and this Section 19.15, unless and until the Service Provider or the relevant SP Affiliate, as the case may be, has complied with Subsection 19.15(b);

(d) The Service Provider shall not rely upon any Intellectual Property Rights of the Service Provider or its Affiliates that are not included in the licenses granted by the Service Provider or its Affiliates herein or in any other license agreement to prevent or restrict the exercise by the Province of any of the rights granted to the Province pursuant to this Section 19.15;

(e) The Service Provider or the relevant SP Affiliate, as the case may be, will provide to the Province, without charge, all Documentation and Source Materials for any SP Proprietary Software in respect of which the Province has the right to make Modifications under Subsections 19.15(b)(b)(i) and 19.15(b)(iii) and are otherwise required by the Province to exercise its rights in respect of the SP Proprietary Software and SP Affiliate Bespoke Software, as applicable, licensed pursuant to this Section 19.15.

19.16 Post-Termination Maintenance and Support.

Subsequent to termination or expiry of this Agreement, the Service Provider will provide to the Province or its designee, including the Alternate Service Provider, any maintenance and support services that Service Provider provides to its customers generally in respect of the SP Proprietary Software retained and used by the Province pursuant to Section 19.15 (*SP Proprietary Software –License to Province after Term and Related Matters*) provided the maintenance and support services are provided for and relate to the version of the SP Proprietary Software retained and used by the Province, on the Service Provider's normal commercial terms and rates for such maintenance and support services or on such other terms as may be agreed between the Province and the Service Provider.

19.17 Use of Confidential Information in Licensed Rights.

The Parties agree that when one Party (the "**Licensor Party**") has granted a Software license to the other Party (the "**Licensee Party**") under this Agreement which provides the Licensee Party with any license rights to the SP Proprietary Software, Province Proprietary Software, or any Modifications thereto (each "**Proprietary Software**"), then the Licensee Party will be entitled to disclose or permit disclosure of that Proprietary Software, to the extent necessary and only insofar as disclosure is necessary on a needs to

know basis, in order for the Licensee Party to exercise its rights under and in accordance with any licences granted by the Licensor Party to the Licensee Party under this Agreement.

19.18 Third Party Notices of Infringement or Requests.

If either Party receives a notice of infringement, request for disclosure, subpoena, or other inquiry with respect to any matter under this Article 19 (*Intellectual Property and Propriety Rights*), then such Party will, as soon as practical, notify the other Party in writing and the matter will be dealt with in accordance with Article 25 (*Indemnification, Liability and Guarantees*). Neither Party will respond to such notices, requests, subpoenas or inquiries, or disclose the other Party's Confidential Information to third parties, without first so notifying the other Party in writing (to the extent possible).

ARTICLE 20 – PROVINCE SHARED INFRASTRUCTURE

20.1 Ownership and Control of Province Shared Infrastructure.

The Parties acknowledge that the Service Provider requires access to and use of the Province Shared Infrastructure during all or a portion of the Term to support the delivery and performance of the Services as contemplated in this Agreement. In connection therewith, the Service Provider acknowledges that:

(a) the Province Shared Infrastructure will at all times be owned, operated and maintained by the Province or on behalf of the Province by third party Persons;

(b) the Service Provider has no ownership or other interest in the Province Shared Infrastructure other than the rights of access to, and use of, the Province Shared Infrastructure granted to the Service Provider under this Article 20 (*Province Shared Infrastructure*) for purposes of delivering and performing the Services in accordance with this Agreement; and

(c) subject to the rights of the Service Provider specifically set out in this Article 20 (*Province Shared Infrastructure*) and otherwise in this Agreement, the Province will have control of, access to and use of the Province Shared Infrastructure, and the sole control of the operation and maintenance of the Province Shared Infrastructure including changes, modifications and upgrades thereto, without requirement for consent of or Approval from the Service Provider.

20.2 Use of Province Shared Infrastructure.

The Province will make available to the Service Provider such access to and use of the Province Shared Infrastructure as is required by the Service Provider to deliver and perform the Services in accordance with this Agreement. Such access and use will be available for the period commencing on the Hand-Over Date (or commencing on such other date as may be agreed to by the Parties during the Term if access to the Province Shared Infrastructure is not required on the Hand-Over Date), to and including the end of the Termination Date or the expiry of the Termination Assistance Period, which ever is the later, or such shorter period of use as may be required by the Service Provider (the "**Shared Infrastructure Use Period**"), and without any additional fee or payment from the Service Provider to the Province unless specifically provided otherwise in this Agreement, or through the Change Order Process. Notwithstanding the foregoing, where the Service Provider is utilizing material portions of the Province Shared Infrastructure, then the Province will advise the Service Provider by written notice of the same, and thereafter the Parties will agree, through the Change Order Process, upon a reasonable apportionment of the actual costs of the Province Shared Infrastructure and maintenance thereof that the Service Provider will pay to the Province (the "**Basic Infrastructure Credit**") in accordance with the provisions of

Section 20.11 (*Basic Infrastructure Credit Payment*). If the parties are unable to agree upon the amount of the Basic Infrastructure Credit, then the determination thereof will be a Dispute and will be settled in accordance with the Dispute Resolution Process under Article 27 (*Dispute Resolution*).

20.3 Restrictions on Access and Use.

The right of the Service Provider to access and use the Province Shared Infrastructure will be subject to the following:

(a) the Service Provider will be given access to and the use of the Province Shared Infrastructure only during the normal hours of operation of the Province Shared Infrastructure during which the same is generally made available to other users thereof. The Province may change and modify such hours of operation from time to time in its discretion, and upon reasonable prior written notice to the Service Provider, provided that:

(i) the Province Shared Infrastructure will be available for use for a reasonable number of hours during each Business Day (and such non-Business Days where the Province Shared Infrastructure is ordinarily made available to its users) and at reasonable hours as may be required to support the delivery and performance of the Services,

(ii) any change or modification of the hours of operation will apply generally to users of the Province Shared Infrastructure and not only or principally to the Service Provider,

(iii) the Service Provider will not be liable for any breach of or failure to perform its obligations under this Agreement, including any failure to meet the Service Levels, to the extent that such breach or failure to perform is attributable to such change or modification of the hours of operation of the Province Share Infrastructure, and

(iv) any decrease in the hours of availability of the Province Shared Infrastructure to the Service Provider (except as may be specifically contemplated as part of the Transformation of the Services under this Agreement) will be made through the Change Order Process;

(b) in exercising its right of access to or use of the Province Shared Infrastructure, the Service Provider will:

(i) not alter, change, damage or remove any furniture, fixtures, equipment, data, information or other matter located at or comprising part of the Province Shared Infrastructure, except with the Approval of the Province, or as specifically contemplated in this Agreement or resulting from the Services provided under this Agreement, and

(ii) following each exercise of access to or use of the Province Shared Infrastructure, leave the Province Shared Infrastructure in substantially the same condition as existed prior to access to or use of the Province Shared Infrastructure by the Service Provider;

(c) the Service Provider will cause all Personnel of the Service Provider or External Personnel used by the Service Provider, in accessing or using the Province Shared Infrastructure, to:

(i) comply with all policies, rules and regulations that the Province may adopt from time to time in respect of the Province Shared Infrastructure, provided that the Province gives the Service Provider prior written notice thereof, and

(ii) at all times and in all circumstances to identify themselves as employees, agents, contractors or representatives of the Service Provider, as applicable, and not as employees, agents, contractors or representatives of the Province;

(d) the Service Provider will access and use the Province Shared Infrastructure only for the purpose of delivering and performing the Services under this Agreement, and for no additional, ancillary or other purpose unless specifically authorized in writing by the Province;

(e) the Service Provider will advise the Province of any intended reduction in use of the Province Shared Infrastructure as soon as the Service Provider is reasonably aware of the same, including any determination by the Service Provider to discontinue all or partial use of the Province Shared Infrastructure, provided that in no event is the Service Provider required to provide more than twelve months' notice of any intended reduction;

(f) to the extent that the Service Provider has any reason to believe that its use of the Province Shared Infrastructure will adversely affect the general operation of the Province Shared Infrastructure (including, without limitation, due to volume or usages changes), then the Service Provider will immediately advise the Province of the same and take all steps as directed by the Province to ensure that any adverse impact on the Province Shared Infrastructure is minimized or eliminated (recognizing that the Province uses the Province Shared Infrastructure to deliver a number of critical services within the Province, and accordingly, the minimization or elimination of any such adverse impact is paramount); and

(g) nothing in this Article 20 (*Province Shared Infrastructure*) entitles the Service Provider to require the Province to change, modify or upgrade the Province Shared Infrastructure.

20.4 Ordinary Course Changes to Province Shared Infrastructure.

The Province, in its sole discretion and from time to time, may make non-material changes, modifications, additions or upgrades to the Province Shared Infrastructure or discontinue use of any non-material portion of the Province Shared Infrastructure in the ordinary course of operations (collectively, "**Ordinary Infrastructure Changes**"), without requirement for the consent of the Service Provider and without prior notice to the Service Provider; provided that the Ordinary Infrastructure Changes do not materially affect or impact the access to and use of the Province Shared Infrastructure by the Service Provider for the delivery and performance of the Services in accordance with this Agreement. If as a result of any Ordinary Infrastructure Changes made, the Service Provider is required to change, modify or upgrade its Systems and operations in order to continue to have access to and use of the Province Shared Infrastructure, then the Service Provider will be solely responsible for making all such changes, modifications or upgrades and for all costs thereof to the Service Provider.

20.5 Material Changes to Province Shared Infrastructure.

The Province may make material changes, modifications, additions or upgrades to the Province Shared Infrastructure or discontinue use of any material portion of the Province Shared Infrastructure from time to time (the "**Material Infrastructure Change**"), notwithstanding that the Material Infrastructure Change may have a material adverse effect or impact on the access to and use of the Province Shared Infrastructure by the Service Provider, provided that:

(a) subject to the Service Provider implementing any changes, modifications, additions or upgrades to its Systems and operations as contemplated in this Section, the Service Provider will continue to have access to and use of the Province Shared Infrastructure to the extent that the Province Shared Infrastructure continues to be operated by the Province; and

(b) the Province will give reasonable prior written notice to the Service Provider of the details of the Material Infrastructure Change, including the analysis of the Province as to the effect and impact of the Material Infrastructure Change to the Service Provider, to the extent known, in the delivery and performance of the Services pursuant to this Agreement.

Where a Material Infrastructure Change may be reasonably expected to have a material adverse effect or impact on the Service Provider, the Province will provide the notice of the Material Infrastructure Change to the Service Provider sufficiently in advance of the implementation thereof so as to afford the Service Provider a reasonable opportunity to make the required changes, modifications, additions and upgrades to its Systems and operations prior to such implementation. The Service Provider will be solely responsible for making all such required changes, modifications and upgrades that may be required as a result of the Material Infrastructure Change, and any material adverse impact suffered or incurred by the Service Provider as a result thereof will be addressed by the Parties through the Governance Process or the Change Order Process. For greater clarification, the Province may discontinue use of any portion of the Province Shared Infrastructure pursuant to this Section where any managed applications of the Service Provider running on the Province Shared Infrastructure cause process loops, runaway jobs, extreme load conditions or other similar adverse impacts to users of the Province Shared Infrastructure, in which case any material adverse impact suffered or incurred by the Service Provider in respect thereof will be at the sole cost of the Service Provider, and will not be addressed by the parties pursuant to the Governance Process or the Change Order Process.

20.6 Changes Required for the Service Provider.

Where a change to the Province Shared Infrastructure is required for the continued access to and use of the Province Shared Infrastructure by the Service Provider (such as a change to accommodate increased demand or capacity), then the following will apply:

(a) the Service Provider will notify the Province, in writing, where a change to the Province Shared Infrastructure is required for the continued access to and use of the Province Shared Infrastructure by the Service Provider, which notice will include a detailed description of all business and technical requirements relating to such requested change, to the extent known;

(b) the Province will review and consider any change to the Province Shared Infrastructure as may be reasonably requested by the Service Provider, having regard to all of the surrounding circumstances including, without limitation, the impact on and the interests of the other users of the Province Shared Infrastructure, and the Province will implement any such changes as may be Approved by the Province;

(c) the Province will prepare a plan, with the assistance of the Service Provider as may be necessary, for the implementation of any such required or requested change will include a detailed description of each change to the Province Shared Infrastructure proposed to be made, and a forecast of any increase to the operating and maintenance costs of the Province in respect of the Province Shared Infrastructure as a result from such change, all to the extent known or reasonably anticipated;

(d) the Province will incorporate all reasonable comments and suggestions as the Service Provider may provide to the Province in writing provided that, for greater clarification, the Province will, at all times, have and retain the sole right to determine the appropriate plan and actions to implement such required or requested change; and

(e) the costs incurred by the Service Provider, if any, as a result of any change to the Province Shared Infrastructure under this Section 20.6 (*Changes Required for the Service Provider*), shall be addressed through the Change Order Process.

20.7 Changes Initiated by the Service Provider.

Where a change to the Province Shared Infrastructure is initiated by the Service Provider, then the following will apply:

(a) the Service Provider may request a change to be made to the Province Shared Infrastructure by notice in writing to the Province which notice will include a detailed description of all business and technical requirements relating to such requested change, to the extent known;

(b) the Province will review and consider any change to the Province Shared Infrastructure as may be reasonably requested by the Service Provider from time to time, having regard to all of the surrounding circumstances including, without limitation, the impact on and the interests of the other users of the Province Shared Infrastructure, and will implement any such changes as may be Approved by the Province;

(c) unless the Service Provider has given notice to the Province that the Service Provider will prepare the plan for the implementation of any such required or requested change, the Province will, at the cost of the Service Provider, prepare a plan for such change and will provide such plan to the Service Provider for its review and consideration;

(d) the plan for the implementation of any such required or requested change will include a detailed description of each change to the Province Shared Infrastructure proposed to be made, as well as a budget of costs anticipated to be incurred to effect and implement such change, and a forecast of any increase to the operating and maintenance costs of the Province in respect of the Province Shared Infrastructure as a result from such change, all to the extent known or reasonably anticipated;

(e) the Province will incorporate all reasonable comments and suggestions as the Service Provider may provide to the Province in writing provided that, for greater clarification, the Province will, at all times, have and retain the sole right to determine the appropriate plan and actions to implement such required or requested change and will have the right to grant the final Approval thereof;

(f) if the Service Provider does not agree with the proposed plan or implementation of the proposed change to the Province Shared Infrastructure, or of the estimated costs or

forecast thereof as provided by the Province to the Service Provider, then matter will be deemed to be a Dispute and will be settled in accordance with the Dispute Resolution Process under Article 27 (*Dispute Resolution*); and

notwithstanding the foregoing, and for greater clarification, the Province will not require the Approval of the Service Provider to the plan in respect of or the implementation of any such required or requested change to the Province Shared Infrastructure and may proceed with such plan and the implementation of such change notwithstanding initiation by the Service Provider of a Dispute pursuant to paragraph (f) above.

20.8 Cooperation of the Parties.

The Parties will cooperate with each other and will use reasonable efforts to make and implement any change, modification or upgrade to the Province Shared Infrastructure determined or Approved by the Province contemplated in this Article 20 (*Province Shared Infrastructure*), including testing of such change, modification or upgrade.

20.9 Change Order Process.

Unless specifically provided otherwise in this Article 20 (*Province Shared Infrastructure*), the change process set forth in Section 20.6 (*Changes Required or Initiated by Service Provider*) and Section 20.7 (*Changes Initiated by Service Provider*), is in lieu of the Change Order Process with respect to the Province Shared Infrastructure.

20.10 Failure of Province Shared Infrastructure.

In the event of an unanticipated failure of the Province Shared Infrastructure, or the occurrence of any unanticipated event or circumstance which prevents the Service Provider from having access to and use of the Province Shared Infrastructure, as is required by the Service Provider for the delivery and performance of the Services, whether arising from the negligence or fault of the Province or otherwise, the Province and the Service Provider acknowledge and agree that:

(a) the Province will have no liability or obligation to the Service Provider in respect thereof other than the obligation to use reasonable efforts and to act with due diligence to correct such failure, or to restore such access to and use of, the Province Shared Infrastructure as soon as reasonably practicable; and

(b) to the extent that the Service Provider is not able to deliver or perform a Service in the manner or to the Service Level required under this Agreement, or to perform any other obligations under this Agreement, as a result of such failure or lack of access to or use of the Province Shared Infrastructure, the Service Provider will be released of all consequences otherwise provided in this Agreement in respect of such failure to deliver and perform such Service, to meet such applicable Service Level or to perform such obligations under this Agreement, until such failure or lack of access to or use of the Province Shared Infrastructure is rectified or remedied to a degree that the Service Provider is able to deliver and perform the Services, and to perform its obligations in accordance with this Agreement.

20.11 Basic Infrastructure Credit Payment.

Where the Service Provider is required by this Article 20 (*Province Shared Infrastructure*) to pay to the Province a Basic Infrastructure Credit or any other payment relating to the Province Shared Infrastructure, then the following provisions will apply:

(a) the Service Provider will make such payment by recording, in favour of the Province, a credit against the Fees payable to the Service Provider under this Agreement, which credit will be applied on a monthly basis, to the extent applicable;

(b) the Province may, at any time, direct the Service Provider not to record a Shared Infrastructure Credit in favour of the Province in respect of an amount payable by the Service Provider to the Province pursuant to this Article 20 (*Province Shared Infrastructure*), and instead to pay such amount to a third party as may be designated by the Province, in which event, the Service Provider will pay such amount to the third party as directed by the Province, and will not record such amount as a credit in favour of the Province. In such event, receipt of payment of such amount by the third party will, and will be deemed to be, receipt of payment of the amount by the Province for all purposes of this Agreement; and

(c) if the Service Provider fails to comply with the preceding provisions of this Section in respect of an amount payable by the Service Provider to the Province under this Article 20 (*Province Shared Infrastructure*), the Province may, by notice in writing to the Service Provider, set-off such amount payable by the Service Provider against any Fees payable by the province to the Service Provider under this Agreement.

20.12 Indemnity.

Notwithstanding any other provision contained in this Article 20 (*Province Shared Infrastructure*), and in addition to any other indemnities provided by the Service Provider to the Province pursuant to this Agreement, the Service Provider hereby indemnifies and agrees to hold harmless the Province and its employees, agents and representatives, to the fullest extent permitted by law, from and against any and all Claims suffered or incurred by any of them arising out of or in connection with the access to and use of the Province Shared Infrastructure by the Service Provider, excepting liability arising out of the independent acts or omissions of the Province, its agents and contractors.

20.13 Termination of Rights to Province Shared Infrastructure.

The Service Provider acknowledges and agrees that its rights in respect of the Province Shared Infrastructure under this Article 20 (*Province Shared Infrastructure*) will cease upon the expiry (or earlier termination in accordance with this Article 20 (*Province Shared Infrastructure*)) of the Shared Infrastructure Use Period. Upon such expiry, the Service Provider will return to the Province all passwords, access codes, access cards and devices of any kind used to obtain access to and use of the Province Shared Infrastructure. For greater clarification, if the Province discontinues use of any portion of the Province Shared Infrastructure, then upon the discontinuance thereof the Service Provider's rights in respect of the discontinued portion of the Province Shared Infrastructure under this Article 20 (*Province Shared Infrastructure*) will cease, and the Service Provider will return to the Province all passwords, access codes, access cards and devices of any kind used to obtain access to and use of the discontinued portion of the Province Shared Infrastructure.

ARTICLE 21 – OTHER COMMERCIAL TERMS

21.1 Growth and Marketing.

The Parties will market and otherwise deal with any potential customers of the Services and the Stakeholders, and will otherwise undertake growth and marketing activities in respect of the Services, in accordance with **Schedule 26** *(Growth and Marketing)*.

21.2 Gainsharing.

The Parties will comply with, and hereby agree to, the gainsharing provisions and principles set forth in the attached **Schedule 27** *(Gainsharing)*.

ARTICLE 22 – AUDIT RIGHTS

22.1 Access Rights.

In connection with the Province's exercise of its rights under this Article 22 (*Audit Rights*), during the Term, and for a period of seven (7) years after the end of the Term, upon prior written request of the Province, except where such prior notice is not required pursuant to the express provisions of this Article 22 (*Audit Rights*) or any other express provisions of this Agreement, the Service Provider will provide the Province and its auditors and other authorized representatives of the Province with access to the following including, where applicable and practicable to do so, with electronic access, to:

(a) all the Province Records or Personal Information related to the Services then in the Custody of the Service Provider, wherever maintained;

(b) any System that contains such Province Records or Personal Information related to the Services, wherever maintained; and

(c) any property or facility at which the Services are being performed, where any such Systems are housed, or where any such Province Records or Personal Information are maintained or stored.

The provisions of Section 22.7 (*General Principles*) will apply with respect to the access rights granted to the Province under this Section.

22.2 Examinations and Copies.

During the Term, upon the prior written request of the Province, the Service Provider will permit the Province and its auditors and their respective authorized representatives, during business hours or such other time as the Parties mutually agree, to examine and make copies of any computer-stored data, correspondence, accounting procedures and practices, and any other relevant supporting financial or operational data including, without limitation, invoices, payments, claims and receipts, and in all cases pertaining to the Services, which will be made available by the Service Provider to the Province and its auditors, and their respective authorized representatives, in British Columbia. Both Parties acknowledge and agree that nothing in this Section will in any way limit or restrict the confidentiality obligations as set forth in Article 16 (*Privacy, Security and Confidentiality*) or as otherwise contemplated by this Agreement.

22.3 Inspection and Investigation Rights.

In the event of a breach or a perceived breach of this Agreement, the Province will have the right, at any time and without prior notice to the Service Provider, either directly or through its representatives, to inspect all or any matters in respect of the Services performed by or on behalf of the Service Provider under this Agreement. The Province will make reasonable efforts in exercising such right of inspection or investigation to not hinder or interfere with the performance of the Services by the Service Provider under this Agreement. For greater clarification, the Province acknowledges that to the extent that any such exercise of the Province's right of inspection or investigation directly hinders or interferes with the Service Provider's ability to deliver Services under this Agreement, then the Service Provider will not be responsible for any Service failure resulting therefrom. The Service Provider will provide the Province and its representatives with all reasonable assistance in connection with any such inspections and investigations. The provisions of Section 22.7 (*General Principles*) will apply with respect to the inspection or investigation rights granted to the Province hereunder.

22.4 Audit Rights.

The Province may appoint an internal or external auditor or other professional advisor at any time and from time to time, but subject to the provisions of 22.7 *(General Principles)*, to review and confirm or verify, in respect of any Contract Year, any aspect of this Agreement and the Services performed under this Agreement including, without limitation, the following:

(a) any matter related to the operational aspects of this Agreement and the Services including, without limitation, to certify or verify:

(i) the integrity of the Province Records or Province Confidential Information including, without limitation, the completeness, accuracy, timelines, confidentiality, availability and security in respect thereof;

(ii) the privacy and security processes of the Service Provider and its Access Subcontractors, and the compliance of the Service Provider and its Access Subcontractors with the Privacy Obligations;

(iii) the general controls, practices, and procedures utilized by the Service Provider in connection with the Services performed;

(iv) the stability and security of the Systems and processes utilized by the Service Provider in performing the Services;

(v) the integrity of all reports provided by the Service Provider to the Province (including the raw data from which such reports are compiled);

(vi) that the Services are being provided in accordance with the terms of this Agreement (including the Service Levels), and in accordance with all Applicable Laws, the Province Policies and any applicable requirements of any regulatory body or authority having competent jurisdiction; and

(vii) the reviews and audits referred to in Article 17 (*Business Continuity and Disaster Recovery*) in respect of the Business Continuity Plan and Disaster Recovery Plan;

(b) any matter related to the financial or business aspects of this Agreement, including verifying the accuracy of all Fees or other amounts invoiced to, or paid by, the Province, the accuracy of financial information provided by the Service Provider to the Province in respect of the calculation of Fees or other amounts invoiced to the Province or set forth in any Proposal in connection with the Change Order Process, or any credits or reductions against the Fees (whether or not properly granted as required by the Service Provider to the Province), and the accuracy of any reporting by the Service Provider to the Province in connection with the foregoing;

(c) operational and other audits requested or otherwise required to be undertaken by the Office of the Comptroller General or the Office of the Auditor General of the Province under the *Financial Administration Act* or any other Applicable Laws regarding any aspect of this Agreement (including, without limitation, an audit of the compliance by the Service Provider with the requirements of this Agreement), or any audits that may be required by Cabinet or Treasury Board of the Province; or

(d) such other audits relating to this Agreement, the obligations of the Service Provider under this Agreement, or the Services as the Province may determine from time to time.

For greater clarification, the Province may, in connection with the exercise of its audit rights pursuant to this Section 22.4 (*Audit Rights*), exercise or cause the Service Provider to exercise rights in respect in this Section.

22.5 Costs.

The costs of any inspections, investigations and audits will be dealt with in accordance with the following provisions:

(a) except as set forth in paragraph (b) below, the Province will pay its costs and expenses of any investigations and inspections under Section 22.3 (*Inspection and Investigation Rights*), and the costs and expenses of any auditor or other professional advisor retained by the Province to conduct or assist with an audit under Section 22.4 (*Audit Rights*) or Section 22.6 (*SysTrust Report*). The Service Provider will pay, and will not seek reimbursement from the Province, for the Service Provider's (or its Subcontractors') costs incurred in connection with any inspection or investigation under Section 22.3 (*Inspection and Investigation Rights*), or any audit conducted pursuant to Section 22.4 (*Audit Rights*) or Section 22.6 (*SysTrust Report*), including the cost of the time and effort of the Service Provider and its Personnel, Subcontractors and External Personnel to comply with the requests and requirements of an inspector, investigator, auditor or other professional advisor in respect of the same; and

(b) where an investigation, inspection or audit reveals a material Deficiency (as determined by the Province, acting reasonably) as a result of the acts or omissions of the Service Provider (or of those Persons for whom the Service Provider is responsible at law or pursuant to the terms of this Agreement), the following provisions will apply:

(i) the Service Provider will resolve such Deficiency in accordance with the provisions of Section 22.8 (*Deficiencies*), and

(ii) upon correction of the material Deficiency so identified, and if so requested by the Province, the Service Provider will undertake a new audit, at the Service Provider's expense, to confirm that such material Deficiency has been fully

addressed and remedied. The Service Provider will promptly provide the results of such audit to the Province upon the Service Provider's receipt of the same.

22.6 SysTrust Report.

The Province may from time to time conduct a "Trust Services Principles and Criteria" examination as governed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (the "**SysTrust Report**") or a Canadian Institute of Chartered Accountants Section 5970 examination (the "**5970 Report**"), in respect of the Services being provided under this Agreement. The SysTrust Report or 5970 Report will report on controls throughout a Contract Year. The SysTrust Report or 5970 Report will be deemed to be an audit for the purposes of this Article 22 (*Audit Rights*) with costs, Deficiency correction and all other matters addressed in the manner as set forth in this Article 22 (*Audit Rights*) for audits.

22.7 General Principles.

In connection with the access, inspection, investigation and audit rights granted to the Province and other Persons under this Article 22 (*Audit Rights*):

(a) the auditors, investigators, inspectors or representatives of the Province will be qualified and trained to levels appropriate to conduct audits, inspections or investigations being conducted;

(b) the Province will cause all such audits, inspections and investigations to be performed during the normal business hours for the Services in question, and upon reasonable prior notice to the Service Provider, other than for inspections or investigations pursuant to Section 22.3 (*Inspection and Investigation Rights*) which may be performed at any time without notice;

(c) the Province will, and will cause its auditors, investigators, inspectors or representatives to:

(i) use reasonable efforts not to hinder or interfere with the performance of the Services by the Service Provider, and for greater clarification, the Province acknowledges that to the extent any such exercise of rights directly hinders or interferes with the Service Provider's ability to deliver the Services, then the Service Provider will not be responsible for any resulting Service Level failures in respect thereof, and

(ii) comply with all security and other similar policies of the Service Provider while at its premises, provided that the Service Provider provides the Province with reasonable prior notice thereof, and provided further that any such security or other similar polices of the Service Provider do not unduly hinder or interfere with the conduct of the audit, inspection or investigation in question;

(d) the Service Provider will, and will cause its Personnel, Subcontractors and External Personnel to:

(i) cooperate with any such inspections, investigations and audits performed by the Province through the Province's auditors, investigators, inspectors or representatives,

(ii) make available on a timely basis the information and Records requested by the Province or its auditors, investigators, inspectors or representatives, and

(iii) provide the Province and its auditors, investigators, inspectors or representatives with assistance in obtaining access to such information and Records, and to any Subcontractors, Personnel or External Personnel, as may be reasonably requested;

(e) the access rights provided for with respect to the premises of the Service Provider will also extend to those premises at which Province Confidential Information, Province Records or Personal Information is stored, and the Service Provider will obtain such corresponding rights from its Subcontractors as may be necessary to give effect to this provision;

(f) the Service Provider will be given the opportunity to respond to the audit, inspection or investigation results before they are finalized, except where it is not reasonably possible or appropriate, as determined by the Province; and

(g) electronic access to any System contemplated in Section 22.1 (*Access Rights*), which contains Province Records or Personal Information in connection with the Services and the records of third parties shall be supervised by the Service Provider.

22.8 Deficiencies.

Following delivery to the Service Provider of an audit, inspection or investigation report that outlines accounting or other Deficiencies of the Service Provider, the Parties will meet as soon as possible through the Governance Process in order to discuss and resolve such Deficiencies. In connection therewith, the following provisions will apply:

(a) if the report identifies the potential for any Deficiency, then the Service Provider will provide the Province, through the Governance Process, with the Service Provider's assessment of the impact of the potential Deficiency;

(b) subject to any alternative agreement reached between the Parties through the Governance Process, the Service Provider will, as soon as reasonably possible (but in any event within thirty (30) days), develop and present to the Province, through the Governance Process, a corrective action plan outlining the timely corrective action that has been taken, or will be taken, by the Service Provider to remedy the Deficiencies;

(c) the corrective action plan will include a sufficient level of detail to allow the Province to assess the appropriateness of the corrective action and plan, including a description of the Deficiency, the specific action to be taken, and a specific implementation schedule that specifies dates and Persons responsible for taking, or who have already taken, the corrective action;

(d) the Province will be given the opportunity, through the Governance Process, to provide the Service Provider with any comments that the Province may have on the corrective action plan, and the Service Provider will take all such comments received by the Province into consideration; and

(e) the Service Provider will remedy the Deficiencies in accordance with the corrective action plan, provided that the Service Provider will be entitled to remedy any Deficiencies that

that are not material in nature, or that do not involve access, use or disclosure of Personal Information, in the ordinary course of business.

ARTICLE 23 – GENERAL DUTIES AND OBLIGATIONS

23.1 General Duties and Obligations of Service Provider.

At all times during the Term and without limiting the other provisions set forth in this Agreement, the Service Provider agrees to, and to cause its directors, officers, Personnel, Affiliates, Subcontractors and all External Personnel to, perform its obligations under this Agreement and to deliver the Services as follows:

(a) in compliance with all of the terms and conditions of this Agreement and all other documents referenced in this Agreement;

(b) in a manner that is consistent with the Parties' objectives set out in Section 1.13 (*Objectives of the Parties*);

(c) in accordance with the standard of care set forth in Section 4.4 (*Standard of Care*);

(d) in accordance with any Change Orders and any agreements made between the Parties pursuant to the Governance Process;

(e) in compliance with all applicable Province Policies which have been provided or otherwise communicated by the Province to the Service Provider from time to time, and in accordance with the Change Order Process; and

(f) in compliance with all Applicable Laws.

23.2 Compliance with Specific Laws.

Without limiting the foregoing Section 23.1 (*General Duties and Obligations of Service Provider*), at all times during the Term, and in the performance of the Services under this Agreement, the Service Provider will comply with, and will cause its Personnel and its Subcontractors and their External Personnel to comply with, those specific Applicable Laws set forth in **Schedule 28** *(Specific Laws and Policies)*, and any other specific Applicable Laws not listed in **Schedule 28** *(Specific Laws and Policies)* but which otherwise apply to the Services given the nature thereof, or any applicable regulations or standards governing the particular industry to which the Services relate. The Service Provider acknowledges that it is familiar with the foregoing as they apply to the Service Provider or to the Services, as applicable.

23.3 FOIPPA Inspections.

The Service Provider acknowledges that under the *Freedom of Information and Protection of Privacy Act* (British Columbia), the Commissioner has the power to obtain information and evidence from persons other than the Province in the course of conducting an investigation or an inquiry under that Act. Accordingly, the Service Provider will cooperate with respect to investigations or inquiries of the Commissioner under that Act regarding Province or Personal Information related matters, and in respect of any information to which the Commissioner is entitled to under such Act.

23.4 Licenses and Permits.

At all times during the Term, the Service Provider will, at its own cost, obtain and maintain in full force and effect all licenses and permits issued by any Governmental Authority which are required or desirable for the proper performance of the Services, or otherwise required or desirable for the performance and completion of the transactions contemplated in this Agreement.

ARTICLE 24 – REPRESENTATIONS, WARRANTIES AND COVENANTS

24.1 Province Representations and Warranties.

The Province represents, warrants and covenants as follows to the Service Provider, as of the date of this Agreement and throughout the Term, and acknowledges and confirms that the Service Provider is relying upon such representations, warranties and covenants in entering into this Agreement:

(a) the Province has the power and authority to enter into, execute and deliver this Agreement and the other Transaction Documents, which have been duly executed and delivered by the Province, and each constitutes a legal, valid and binding obligation of the Province enforceable against it in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunction are equitable remedies available only in the discretion of the court;

(b) the Province has the power and authority to perform its obligations under this Agreement and the other Transaction Documents as contemplated in this Agreement; and

(c) neither the execution and delivery of this Agreement, the other Transaction Documents, nor the compliance with the terms thereof by the Province:

(i) has resulted or will result in a violation of any Applicable Laws, or

(ii) requires the Approval or consent of any Person or any Governmental Authority except such as has been obtained as of the date of this Agreement.

24.2 Service Provider Representations, Warranties and Covenants.

The Service Provider represents, warrants and covenants as follows to the Province, as of the date of this Agreement and (except as otherwise noted) throughout the Term, and acknowledges and confirms that the Province is relying upon such representations, warranties and covenants in entering into of this Agreement:

(a) the Service Provider is a corporation duly incorporated and validly existing under the laws of British Columbia and is in good standing with respect to the filing of annual returns thereunder;

(b) all of the issued and outstanding common shares in the capital of the Service Provider are registered in the name of the EDS Canada Inc., and EDS Canada Inc. is the legal and beneficial owner thereof and the one issued and outstanding special share in the capital of the Service Provider is registered in the name of the Province, and the Province the legal and beneficial owner thereof.

(c) the Performance Guarantor is a company duly incorporated and validly existing under the laws of Canada and is in good standing with respect to the filing of annual returns thereunder;

(d) the Performance Guarantor and the Corporate Guarantor are affiliated companies;

(e) the Corporate Guarantor is a publicly-held company duly incorporated and validly existing under the laws of Delaware and listed on the New York Stock Exchange;

(f) the Service Provider has, and throughout the Term will maintain, its registered office within the Province of British Columbia;

(g) all of the Service Provider's directors are Canadian citizens and resident in Canada;

Power, Capacity and Legal Authority

(h) the Service Provider has all necessary corporate power, capacity and legal authority to enter into, execute and deliver this Agreement and the Transaction Documents to which it is a party, and to perform its obligations under this Agreement and such Transaction Documents, and this Agreement and such Transaction Documents have been duly executed and delivered by the Service Provider, and each constitutes a legal, valid and binding obligation of the Service Provider enforceable against the Service Provider in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

(i) the Performance Guarantor has all necessary corporate power, capacity and legal authority to enter into, execute and deliver the Performance Guarantee and to perform its obligations thereunder, and the Performance Guarantee has been duly executed and delivered by the Performance Guarantor, and constitutes a legal, valid and binding obligation of the Performance Guarantor enforceable against the Performance Guarantor in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

(j) the Corporate Guarantor has all necessary corporate power, capacity and legal authority to enter into, execute and deliver the Corporate Guarantee and to perform its obligations thereunder, and the Corporate Guarantee has been duly executed and delivered by the Corporate Guarantor, and constitutes a legal, valid and binding obligation of the Corporate Guarantor enforceable against the Corporate Guarantor in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

No Violation

(k) neither the execution and delivery of this Agreement and the other Transaction Documents, nor the compliance with the terms of this Agreement and the other Transaction Documents by the Service Provider:

(i) has resulted or will result in a violation of any Applicable Laws,

(ii) has resulted or will result in a breach of, or constitute a default under, the Service Provider's constating documents, any shareholders' agreement to which it is a party, or any shareholder or directors' resolutions,

(iii) has resulted or will result in a breach of, or constitute a default under, any instrument or agreement to which the Service Provider is a party or by which the Service Provider is bound, or

(iv) requires the Approval or any consent of any Person or any Governmental Authority except such as has been obtained as of the date of this Agreement;

Permits, Approvals and Operating Matters

(l) the Service Provider holds, and will hold as of the Hand-Over Date and throughout the Term, all material permits, approvals, authorizations and consents that may be required from any Person or Governmental Authority in order for the Service Provider to perform its duties and obligations pursuant to the terms of this Agreement and to provide the Services as contemplated under this Agreement, and the Service Provider is, and at the Hand-Over Date and throughout the Term will be, in good standing with respect to all such permits, approvals, authorizations and consents, and none of the same contain, or will contain, any term, provision, condition or limitation which would have a material adverse effect on, or materially adversely restrict or impair the performance by, the Service Provider of its duties and obligations under this Agreement or the performance of the Services pursuant to the terms of this Agreement;

(m) the Service Provider has filed all tax, corporate information and other returns required to be filed under all Applicable Laws, has complied with all workers compensation legislation and other similar legislation to which it may be subject, and has paid all Taxes, fees and assessments calculated to be due by it under those laws as of the date of this Agreement;

(n) the Service Provider has, and throughout the Term will maintain, sufficient and appropriate assets and Personnel to enable the Service Provider to perform and fulfill its obligations under this Agreement and to perform the Services in accordance with the terms of this Agreement;

Intellectual Property, Systems and Assets

(o) the performance by the Service Provider of the Services under this Agreement, and all of the Systems, Software and other Intellectual Property utilized by the Service Provider in the delivery of the Services (other than Intellectual Property licensed by the Province to the Service Provider pursuant to Section 19.9 (*Use of Province Licensed Software*)) does not and will not violate or infringe, or constitute a misappropriation of, the Intellectual Property or rights of any Person;

(p) all Systems used by the Service Provider or its Subcontractors will be maintained by the Service Provider or its Subcontractors in good working order, ordinary wear and tear excepted;

(q) all tangible personal assets including hardware that are transferred, assigned or licensed (as applicable in accordance with the terms of this Agreement) by the Service Provider to the Province at any time during the Term and upon the Termination, will be free and clear of all Liens at the time of transfer, assignment or license to the Province, other than the interests of a lessor in respect of any leased assets, or such Liens as may have been granted in respect of such leased assets by the lessor thereof;

(r) at such time as the Service Provider transfers, assigns or licenses any Intellectual Property or Intellectual Property Rights to the Province pursuant to this Agreement, the Service Provider will have all necessary right, title and interest in the Intellectual Property or Intellectual Property Rights to complete such transfer, assignment or license, as the case may be, in accordance with its terms;

Litigation, Proceedings and Limiting Agreements

(s) as of date of this Agreement, there are no suits, actions, proceedings, judgments or orders outstanding or, to the knowledge of the Service Provider, threatened against or affecting the Service Provider or any of its assets by or before any court, tribunal, board or other Governmental Authority that would, if adversely determined, have a material adverse effect on, or materially adversely restrict or impair the performance by, the Service Provider of its duties and obligations under this Agreement or the performance of the Services pursuant to the terms of this Agreement;

(t) as of the date of this Agreement, there are no material labour actions, proceedings, grievances, judgments or orders outstanding or, to the knowledge of the Service Provider, threatened against or affecting the Service Provider by or before any court, tribunal, board or other Governmental Authority, which could have a material adverse effect on, or materially adversely restrict or impair the performance by, the Service Provider of its duties and obligations under this Agreement or the performance of the Services pursuant to the terms of this Agreement;

Insolvency

(u) the Service Provider is not insolvent, is able to pay its debts as they become due in the ordinary course of business, and the entering into of this Agreement and the other Transaction Documents and the performing of its obligations under this Agreement and the other Transaction Documents will not render the Service Provider insolvent or unable to pay its debts as they become due;

Subcontractors and Personnel

(v) attached as **Schedule 20** *(Subcontractor Matters)* is a list of all of the Subcontractors who are required to be Approved by the Province under the provisions of Section 12.11 (*Consent to Use of Material Subcontractors*) with respect to the performance of the Services, as such Schedule may be amended from time to time in order to accurately reflect such Subcontractors during the Term, and all other actions required to be taken with respect to such Subcontractors have been taken including, without limitation, the incorporation in the agreements with such Subcontractors of the required provisions as set forth in Article 12 (*Subcontractors*) and in the Privacy Obligations;

Miscellaneous

(w) as of the date of this Agreement, all information provided by the Service Provider to the Province in the course of responding to the JSRFP prior to entering into this Agreement was true and correct in all material respects and was not intentionally misleading at the time of disclosure, and the Service Provider has not intentionally failed to disclose any further information which failure would make the information previously disclosed misleading;

(x) the Service Provider is under no current obligation or restriction, nor will it knowingly assume any such obligation or restriction that does or could in any way interfere or conflict with, or that does or could present a conflict of interest concerning, the performance of the Service Provider's obligations and the providing of the Services under the terms of this Agreement;

(y) there has been no collusion, relationship with, benefit granted to or benefit received from any other Person with respect to the JSRFP, this Agreement, the delivery of the Services or anything related thereto except:

(i) for subcontracts, teaming agreements and other similar contracts entered into in the ordinary course of business,

(ii) obligations to pay commissions or other incentive compensation in compliance with compensations programs of the Service Provider and its Subcontractors and its or their Affiliates, and

(iii) as otherwise expressly disclosed by the Service Provider to the Province in writing;

(z) the Service Provider has no knowledge of any material fact or matter not disclosed to the Province by the Service Provider which, if known by the Province, might be reasonably expected to deter the Province from entering into this Agreement or completing the transactions contemplated in this Agreement and in the other Transaction Documents, or that might materially adversely affect the ability of the Service Provider to perform its obligations under this Agreement; and

(aa) the Service Provider represents and warrants those matters specifically set forth in **Schedule 29** *(Additional Representations and Warranties)*.

24.3 Disclaimer of Warranties.

Other than the representations and warranties expressly set out in this Agreement or in the other Transaction Documents, neither Party makes any representation or warranty, expressed, implied, statutory or otherwise regarding any matter in connection with this Agreement or the other Transaction Documents including representations or warranties of merchantability or fitness for a particular purpose.

24.4 No Guarantee of Service Volumes.

The Service Provider acknowledges and agrees that the Province makes no representation or warranty as to the nature, timing, quality, quantity or volume of Services required from the Service Provider under this Agreement, or the volume of business or any particular type of transaction or other measurable matter that will be handled by the Service Provider in providing the Services under this Agreement, or the

compensation that may be earned by the Service Provider under this Agreement. The Service Provider acknowledges and agrees that it has conducted its own due diligence prior to entering into this Agreement as to the services performed by or on behalf of the Province historically in connection with the business that will be undertaken by the Service Provider in performing the Services. The Province has advised the Service Provider, and the Service Provider acknowledges, that historic information with respect to the Services or such business, including any particular type of transaction or other measurable matter, may not be representative of the future nature, timing, quality, quantity or volume of Services that will be required under or performed by the Service Provider under this Agreement, or the volume of business or any particular type of transaction or other measurable matter that will be handled by the Service Provider in connection with this Agreement.

ARTICLE 25 – INDEMNIFICATION, LIABILITY AND GUARANTEES

25.1 General Intent.

Each Party will be liable to the other for any damages that may be properly and lawfully awarded against each Party in favour of the other under the terms of, or in connection with, this Agreement. Both Parties agree, however, that monetary damages may not be a sufficient remedy for any breach of this Agreement, and each Party will be entitled to seek equitable relief, including injunctive relief and specific performance in the event of a breach of this Agreement, to the extent that such remedy is available to a Party in accordance with Applicable Laws (including, without limitation, the *Crown Proceeding Act* (British Columbia)), but subject any express limitations otherwise provided for in this Agreement.

25.2 Indemnification by the Service Provider.

The Service Provider will indemnify and save harmless the Province and its employees, advisors, agents and representatives (the "**Province Indemnified Parties**"), to the fullest extent permitted by law, from and against any Claims that may be suffered or incurred by any one or more of the Province Indemnified Parties arising as a result of, or in connection with, any of the matters set forth in Section 1 of **Schedule 30** *(Indemnification Matters)*, except to the extent suffered or incurred as a result of or in connection with the wilful misconduct, fraud, malfeasance or gross negligence of the Province Indemnified Parties.

25.3 Indemnification by the Province.

The Province will indemnify and save harmless the Service Provider and its employees, advisors, agents and representatives (the "**Service Provider Indemnified Parties**"), to the fullest extent permitted by law, from and against any Claims that may be suffered or incurred by any one or more of the Service Provider Indemnified Parties arising as a result of, or in connection with, any of the matters set forth in Section 2 of **Schedule 30** *(Indemnification Matters)*, except to the extent suffered or incurred as a result of or in connection with the wilful misconduct, fraud, malfeasance or gross negligence of the Service Provider Indemnified Parties.

25.4 Third Party Claim Process.

Subject to any restrictions or other limitations contained in the *Crown Proceeding Act* (British Columbia), or other Applicable Laws:

(a) if a Party (an "**Indemnified Party**") intends to seek indemnification under this Agreement from the other Party (the "**Indemnifying Party**") in respect of any third party Claims, then the Indemnified Party will promptly give the Indemnifying Party written notice of such Claims for indemnification, such notice to be given as soon as practicable following the commencement of any action by a third party; provided, however, that the failure of

an Indemnified Party to give the Indemnifying Party such prompt notice will not relieve the Indemnifying Party of its obligations under this Agreement, except to the extent that such failure results in a material prejudice to the Indemnifying Party's defence to such Claims;

(b) if the Indemnifying Party receives a notice of any Claims pursuant to paragraph (a) above, then:

(i) where the Indemnifying Party is the Province, it will have the right to assume the defence of such Claims, at its sole cost and expense, with counsel designated by the Province; and

(ii) where the Indemnifying Party is the Service Provider, the Province will cooperate with the Service Provider and, where appropriate and in the discretion of the Province, will allow the Service Provider to control the defence of the Claim and any related settlement, at the Service Provider's sole cost and expense, it being acknowledged and agreed that where the Province determines that it is not so appropriate, then the Province will control the defence of the Claim and any related settlement;

provided, however, that if the defendants in any such action include both the Indemnified Party and the Indemnifying Party, and the Indemnified Party reasonably concludes that there may be legal defences available to it which are different from or additional to those available to the Indemnifying Party, then the Indemnified Party will have the right to select separate counsel, the cost of which will be at the Indemnified Party's expense (without reimbursement by the Indemnifying Party under an indemnity or otherwise) to assert such legal defences or to otherwise participate in the defence of such action on behalf of the Indemnified Party;

(c) if the Indemnified Party is entitled to indemnification under this Agreement as a result of a Claim by a third party, and if the Indemnifying Party fails or chooses not to assume the defence of such Claim, or fails to proceed, then the Indemnified Party may, at the expense of the Indemnifying Party, contest (or, with or without the prior consent of the Indemnifying Party, settle) such Claim. The Indemnified Party will not otherwise settle any Claim with respect to which it has sought or intends to seek indemnification pursuant to this Agreement without the prior written consent of the Indemnifying Party, which consent will not be unreasonably withheld or delayed; and

(d) if the Indemnifying Party settles any Claims that it may be liable to provide indemnification pursuant to this Section without the prior written consent of the Indemnified Party, which consent will not be unreasonably withheld or delayed (acknowledging that pursuant to the *Crown Proceeding Act* (British Columbia) the Province is not required to obtain or provide such consent, and will not be required to do so pursuant to this provision); then if the Indemnifying Party has reached a *bona fide* full and final settlement in respect of all Claims involving the Indemnified Party and such plaintiff(s) in any such action with the plaintiff(s), and the Indemnified Party does not (or is not asked to) consent to such settlement, the dollar amount specified in the settlement will act as an absolute maximum limit on the indemnification obligation of the Indemnifying Party.

25.5 Mitigation.

Each Party has a duty to mitigate the Claims that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and reasonable actions to reduce or limit the amount of such Claims.

25.6 Limitation on Liability.

The liability of the Parties under this Agreement will be subject to the express terms and conditions set forth in **Schedule 31** *(Limitation on Liability)*.

25.7 Performance Guarantee.

Concurrently with the signing of this Agreement, the Service Provider will provide to the Province a duly executed Performance Guarantee, in the form attached as **Schedule 32** *(Performance Guarantee)*.

25.8 Corporate Guarantee.

Concurrently with the signing of this Agreement, the Service Provider will deliver to the Province a duly executed Corporate Guarantee, in the form attached to this Agreement as **Schedule 33** *(Corporate Guarantee)*.

ARTICLE 26 – INSURANCE

26.1 Insurance.

The Service Provider will procure and maintain at all times during the Term of this Agreement, at its own expense and without reimbursement from the Province, the insurance policies more particularly described in **Schedule 34** *(Insurance)*, which will be underwritten by insurers licensed to carry on insurance business in Canada.

26.2 Certificate of Insurance.

The Service Provider will not cancel any of the required insurance policies set out or contemplated in **Schedule 34** *(Insurance)* without thirty (30) days prior written notice to the Province, and consent of the Province where a cancelled insurance policy is not replaced with a replacement insurance policy of the same kind and type, and in an equal or greater amount. Each insurance policy for the above- described insurance coverage will be endorsed to provide the Province with thirty (30) days prior written notice of cancellation or material change. The Service Provider will provide the Province with reasonable evidence of the obtaining of all insurance required to be obtained by the Service Provider, before commencing any Services under this Agreement. Such evidence will be in the Province's form of insurance certificate, as the same may be amended from time to time by the Province and notified by the province to the Service Provider, a copy of which is attached as **Schedule 35** *(Form of Insurance Certificate)*, unless otherwise agreed to in writing by the Province. The Service Provider will provide similar evidence of the continued existence of all required insurance coverage on an annual basis within thirty days of the renewal of such insurance policies, and upon the request of the Province from time to time.

26.3 Adequacy of Insurance.

The Service Provider acknowledges that any requirement or advice by the Province as to the amount of coverage under any policy of insurance does not, and will not be deemed to, constitute a representation by the Province that the amount required under such insurance is adequate, and the Service Provider

acknowledges and agrees that it is solely responsible for obtaining and maintaining its own policies of insurance in such amounts as the Service Provider will determine to be appropriate and adequate, subject to the minimum requirements set out on **Schedule 34** *(Insurance)*.

ARTICLE 27 – DISPUTE RESOLUTION

27.1 Informal Dispute Resolution.

In the event of any Dispute, the Parties will use reasonable efforts to settle such Dispute internally and will consult and negotiate with each other in good faith in an effort to reach a fair and equitable solution satisfactory to the Parties. Prior to the initiation of formal dispute resolution procedures, the Parties will first attempt to informally resolve any dispute, controversy or Claim (including any failure by the Parties to reach agreement where expressly provided for in this Agreement) arising under or in connection with this Agreement as follows:

(a) the Service Provider STMS Lead and the Province will attempt to resolve the Dispute informally by meeting as often, for a duration and as promptly as those representatives deem necessary, to discuss the Dispute and negotiate in good faith in an attempt to resolve the Dispute;

(b) if such persons are unable to resolve the Dispute within a reasonable period, then either one of them may refer the Dispute to the Joint Executive Committee, and the Joint Executive Committee will promptly schedule a meeting to discuss the Dispute and negotiate in good faith in an attempt to resolve the Dispute;

(c) the Joint Executive Committee will meet as often and as promptly as the Parties deem necessary to discuss the Dispute and negotiate in good faith in an effort to resolve the Dispute;

(d) during the course of all discussions referred to in paragraphs (a) to (c) above, all reasonable requests made by one Party to another for non-privileged information, reasonably related to the Dispute, will be provided by the other Party so that both Parties may be fully apprised of the other's interests in the Dispute and resulting positions and interests. The specific format for such discussions will be decided by mutual agreement of the Parties, but may include the preparation of agreed-upon statements of fact or written statements of position or interest;

(e) if the Joint Executive Committee does not resolve the Dispute within (10) Business Days of the referral of the Dispute to the Joint Executive Committee (or such longer period to which the Parties may agree), then either Party may upon written notice to the other Party (the "**Mediation Notice**") elect to submit the Dispute to non-binding mediation, and if such Mediation Notice is accepted in writing within five (5) Business Days of receipt thereof, then the Parties will proceed to mediation in accordance with paragraph (f) below. For greater clarification, either Party may elect to bypass mediation, in which case, the Dispute will be settled by binding arbitration in accordance with Section 27.2 (*Arbitration*);

(f) if the Dispute is referred to non-binding mediation in accordance with paragraph (e) above, then the Parties will thereafter attempt to promptly agree upon and appoint a sole mediator. If the Parties are unable to agree upon a mediator within five (5) Business Days after the effective date of the Mediation Notice (or such longer period as the Parties may

agree), then the Parties will bypass mediation and proceed to arbitration in accordance with Section 27.2 (*Arbitration*);

(g) if the Parties agree upon a mediator within the time required pursuant to paragraph (f) above, then the mediation will be conducted at a time, in a city in British Columbia and at a specific location as may be agreed to by the Parties with the mediator, or if the Parties cannot agree, as so designated by the mediator. The mediation will be held within five (5) Business Days after the mediator is appointed. If any Party has substantial need for information from another Party in order to prepare for the mediation, then the Parties will use reasonable efforts to agree on procedures for the formal exchange of information. Each Party will be represented in the mediation by at least an individual with authority to settle the Dispute on behalf of that Party and, if desired by that Party, by legal counsel for that Party. The Parties' representatives in the mediation will continue with the mediation as long as the mediator reasonably requests, but in no event longer than thirty (30) days from the first day that the Parties meet to commence mediation. Unless otherwise agreed to in writing by the Parties, each Party will pay one-half of the mediator's fees and expenses and will bear all of its own expenses in connection with the mediation. No Party may employ or use the mediator as a witness, consultant, expert, counsel or other similar position regarding the Dispute or any related matters; and

(h) if the parties are unable to resolve the Dispute by mediation, or if either Party elects to bypass mediation entirely, then the matter will be referred to binding arbitration in accordance with Section 27.2 (*Arbitration*).

27.2 Arbitration.

Subject to the provisions of **Schedule 30** *(Indemnification Matters),* **Schedule 31** *(Limitation on Liability)*, Section 27.3 (*Expedited Arbitration*) and Section 27.44 (*Special Arbitration*), any Dispute that is not settled in accordance with Section 27.1 (*Informal Dispute Resolution*), will be settled at the request of either Party by binding arbitration in Victoria, British Columbia in accordance with the *Commercial Arbitration Act* (British Columbia) on the following terms:

(a) all hearings will be in held and kept confidence;

(b) the arbitration will be heard before one arbitrator, or a panel as determined in accordance with Section 27.6 (*Designated Arbitrators*);

(c) unless the Parties agree otherwise in writing, all arbitrators will either be:

(i) a lawyer in good standing with the Law Society or equivalent body in all jurisdictions in Canada where that lawyer is called to the bar,

(ii) a retired lawyer who was previously in good standing with the Law Society or equivalent body in all jurisdictions in Canada where that lawyer was previously called to the bar before that lawyer's retirement; or

(iii) a retired judge;

(d) no individual may be appointed as an arbitrator if that individual is (but for the appointment as arbitrator in connection with a Dispute under this Agreement) or was directly involved in matters relating to this Agreement, the Dispute or the Services to be performed by the Service Provider under this Agreement;

(e) all arbitrators selected or otherwise appointed to hear a Dispute will have experience in complex, commercial outsourcing engagements and be skilled or knowledgeable in the subject matter of the Dispute;

(f) if the arbitration is heard before a panel of three arbitrators, then the decision of the arbitration panel will be made by a majority vote;

(g) judgment upon the award rendered in any such arbitration may be entered in any court having competent jurisdiction;

(h) the Parties will direct the arbitrator (or arbitrators) to make an award of costs, which award will include the remuneration and expenses and any related administrative fees that are charged by the arbitrator (or arbitrators) in connection with the arbitration of the Dispute, as well as the costs and expenses incurred by each Party in preparing for and participating in the arbitration (including the costs related to retaining legal counsel), and the Parties will pay all such costs in accordance with the direction of the arbitrator (or arbitrators);

(i) the Parties will instruct the arbitrator (or arbitrators) to make the final award with respect to the Dispute within 60 days after the hearings have been closed, or such other reasonable period of time (not to be less than thirty (30) days), as may be agreed to in writing by the Parties before the commencement of the arbitration hearings and so notified in writing to the arbitrator (or arbitrators);

(j) notwithstanding anything to the contrary in the *Commercial Arbitration Act* (British Columbia):

(i) the same procedural requirements and rights of discovery as are available under the British Columbia Rules of Court will apply, *mutatis mutandis*, except that the arbitrator (or arbitrators) may make adjustments to the time limits contained in such Rules of Court,

(ii) the laws and rules of evidence applicable in the Courts of British Columbia will apply, and the arbitrator (or arbitrators) may only require the production of relevant documentary and testimonial evidence not protected by the solicitor-client privilege, and

(iii) the arbitrator (or arbitrators) will adjudicate the Dispute by reference to law in accordance with Section 23 of the *Commercial Arbitration Act* (British Columbia), including the precedent of other Court decisions, statutory laws, and laws of interpretation, as would be followed by a Court having competent jurisdiction, and the Parties expressly agree that the Dispute will not be decided upon the law of equity or some other similar basis;

(k) the arbitrator (or arbitrators) will have no power or authority to grant any award or permit any other recourse that would be precluded by the terms of this Agreement, and nor will the arbitrator (or arbitrators) have the power to make any award that addresses matters outside the scope of the Dispute; and

(l) the Parties will be bound by any award issued by the arbitrator (or arbitrators), which award the Parties agree to be bound by and to accept as a final and binding award.

27.3 Expedited Arbitration.

Certain Disputes are expressly designated as being subject to Expedited Arbitrations under the terms of this Agreement, and in particular, to Section 6.4 (*Disputes Regarding Transformation Plan*) and Section 7.8 (*Implementation of Mandatory Changes*) and as may be specifically provided for in any Schedule to this Agreement or in other Transaction Documents. All such Disputes designated as Expedited Arbitrations shall follow the step-by-step resolution procedures set forth below to the extent necessary to resolve the Dispute, without first having to comply with the provisions of Section 27.1 (*Information Dispute Resolution*) or Section 27.2 (*Arbitration*):

(a) The Expedited Arbitration resolution process shall be commenced by a notice from either Party to the other referring to this paragraph 27.3(a) and setting out the matter that is to be resolved as an Expedited Arbitration and such notice shall constitute the commencement of the Dispute Resolution Process in respect of such Expedited Arbitration;

(b) will attempt to resolve the Dispute informally by meeting as often, for a duration and as promptly as those representatives deem necessary, to discuss the Dispute and negotiate in good faith in an attempt to resolve the Dispute

(c) the Joint Executive Committee shall attempt to resolve any Dispute informally by meeting as often, for duration and as promptly as those representatives deem necessary, but for a period not to exceed three (3) Business Days to discuss the Dispute and negotiate in good faith in an attempt to resolve the Dispute;

(d) if the Joint Executive Committee is unable to resolve the Dispute within three (3) Business Days, then within two (2) Business Days thereafter, the Deputy Minister, Labour and Citizens' Services and the President of EDS, or such other representative of the Parties as may be acceptable to both Parties, shall meet in person or by teleconference at a mutually agreeable time to resolve the Dispute; and

(e) if such persons are unable to resolve the Dispute within such meeting or such successive meetings as agreed to, then either Party may refer to the Dispute to the first Designated Arbitrator who is immediately available, and where no such Designated Arbitrator is immediately available, the first available Designated Arbitrator. The Expedited Arbitration shall be settled by binding arbitration in Victoria, British Columbia in accordance with the *Commercial Arbitration Act* (British Columbia), in the presence of one Designated Arbitrator subject to the following:

(i) submissions being required to be made within twenty (20) Business Days of the arbitrator being appointed,

(ii) the arbitrator being required to render a decision within twenty (20) Business Days of receipt of the submissions, and

(iii) each Party shall pay its own costs and expenses and one-half (1/2) of the arbitrator costs, except in the event of extraordinary or extenuating circumstances where, in the judgment of the arbitrator, having regard to all of the surrounding circumstances, it would be inequitable or otherwise inappropriate to do so, in which case, the Parties shall pay the costs of the arbitrator in accordance with the final apportionment thereof by the arbitrator.

27.4 Special Arbitration.

In the event the Parties decide to resolve certain Disputes by special arbitration, then the Parties will follow the step-by-step resolution procedures set forth in Section 27.1 (*Informal Dispute Resolution*) and to the extent applicable, Section 27.2 (*Arbitration*), provided that the following provisions will apply in respect of any such arbitration:

(a) for purposes of Subsection 27.2(i) (*Arbitration*), the arbitrator (or arbitrators) will be instructed to make an award by selecting the submission of one Party over the other, which selected submission will constitute the award of the arbitrator (or arbitrators, if applicable), provided that any award of costs contained in such submission may be removed by the arbitrator (or arbitrators, if applicable) and replaced with an award of costs determined by the arbitrator (or arbitrators, if applicable) in accordance with the provisions of Subsection 27.2(h) (*Arbitration*);

(b) if any submission includes matters that are outside the scope of the Dispute contemplated then the arbitrator (or arbitrators, if applicable) will discard the submission in its entirety as not being in compliance with the scope of the Dispute, and select the other submission for purposes of paragraph (a) above, and if both submission are discounted in their entirety as a result of the application of the provisions of this paragraph, then the arbitrator (or arbitrators) will instruct the Parties, in writing, to resubmit new submissions without such provisions which are outside the scope of the Dispute; and

(c) for greater clarification, the arbitrator (or arbitrators, if applicable) will not have any jurisdiction, power or authority to grant an award other than as provided for in this Section 27.4 (*Special Arbitration*).

27.5 Confidentiality.

The proceedings of all negotiations, mediations and arbitrations as part of the Dispute Resolution Process will at all times be privately conducted. The Parties agree that all statements and other communications made during the Dispute Resolution Process including, without limitation, offers of settlement, settlement terms and all documents or other materials created for the purposes of the Dispute Resolution Process:

(a) are made on a without prejudice basis;

(b) do not constitute an admission or waiver of rights; and

(c) will not be offered into evidence, disclosed or used for any other purpose other than the Dispute Resolution Process.

During the Dispute Resolution Process, no Party is required to disclose to the other Party any information, documents or materials with respect to which they claim privilege; however, if as part of the Dispute Resolution Process a Party should disclose to the other Party information, documents or materials with respect to which they claim privilege or any information, documents or materials which they regard and identify as confidential or proprietary, then the other Party will maintain the confidentiality of the information, documents or materials so obtained and, to the extent permitted by law, any such disclosure will not constitute a waiver of any privilege or confidentiality. The Parties agree that any information regarding the Dispute Resolution Process, including any decisions or awards made, will not be disclosed to any third parties or used for any purpose other than the Dispute Resolution Process, unless the Parties otherwise agree; provided that nothing in this provision will prevent such disclosure as may be necessary to enforce any arbitration awards.

27.6 Designated Arbitrators.

For the purposes of this Article 27 (*Dispute Resolution*), the Parties agree to select an arbitrator to hear the arbitration of a Dispute from the list of arbitrators set forth in **Schedule 42** (*Designated Arbitrators*), beginning with the arbitrator at the top of the list and moving to the end of the list, as such selection is made pursuant to Section 27.2 (*Arbitration*), Sections 27.3 (*Expedited Arbitration*) or 27.4 (*Special Arbitration*). For greater certainty, if the Person at the top of the list is not available, then the Parties will move to the next Person on the list. The Parties shall review **Schedule 42** (*Designated Arbitrators*), from time to time, but not less than annually, through the Joint Executive Committee and amend or update the list by written agreement of the Parties. In the event that no Persons are available from the list set forth in **Schedule 42** (*Designated Arbitrators*) and the Parties cannot agree upon a Person to act as the Designated Arbitrator, then each Party will select an arbitrator, and those two arbitrators will jointly select a third arbitrator.

27.7 Exceptions to Dispute Resolution Procedure.

The provisions of this Article 27 (*Dispute Resolution*) will not be construed to prevent a Party from:

(a) seeking a temporary restraining order or injunctive or other equitable relief with respect to a breach (or attempted breach) of this Agreement by the other Party, to the extent such remedies are available to a Party pursuant to Applicable Law (including, without limitation, the *Crown Proceeding Act* (British Columbia)); or

(b) instituting litigation or other formal proceedings to the extent necessary and available pursuant to Applicable Law:

(i) to enforce arbitration awards or orders for injunctive or other similar relief,

(ii) to avoid the expiration of any applicable limitations period, or

(iii) to preserve a position with respect to other creditors.

27.8 Continuity of Services.

The Service Provider acknowledges that the timely and complete performance of its obligations pursuant to this Agreement is critical to the business and operations of the Province and the continuity of the Services. Accordingly, in the event of a Dispute, and at all times before, during and after the Dispute Resolution Process:

(a) the Service Provider will continue to so perform its obligations and to deliver the Services under this Agreement in good faith during the resolution of such Dispute; and

(b) the Province will continue to pay all Fees payable to the Service Provider in accordance with the terms of this Agreement, other than those Fees which are in Dispute and withheld from payment in accordance with the provisions of Section 15.6 (*Disputed Payments*).

ARTICLE 28 – DEFAULT AND TERMINATION

28.1 Service Provider Material Breach.

The Service Provider will be in material breach of its obligations under this Agreement upon the occurrence of any one or more of the following events or the events set forth in **Schedule 36** *(Material Breach)* (each a "**Material Breach**"):

(a) an Event of Insolvency in respect of the Service Provider, the Performance Guarantor or the Corporate Guarantor;

(b) if the Service Provider, the Performance Guarantor or the Corporate Guarantor ceases or threatens to cease to carry on business;

(c) any direct or indirect assignment of this Agreement by the Service Provider contrary to the provisions of Section 31.2 (*Assignment by the Service Provider*);

(d) there is, without the Approval of the Province, a corporate or other similar structural reorganization of the Service Provider, the Performance Guarantor or the Corporate Guarantor, except for those corporate or other similar structural reorganizations that:

(i) do not result in a direct or indirect assignment of this Agreement by the Service Provider contrary to the provisions of Section 31.2 (*Assignment by the Service Provider*),

(ii) do not adversely affect the Performance Guarantee or the Corporate Guarantee in any way, or the ability of the Performance Guarantor or the Corporate Guarantor to perform their respective obligations under the Performance Guarantee or the Corporate Guarantee respectively (including, in the case of the Performance Guarantor, to comply with the provisions of the Privacy Obligations), and

(iii) there is no increased risk of a breach of, or an actual breach of, the Privacy Obligations, as determined by the Province in its sole discretion;

(e) any disclosure of Personal Information pursuant to a Disclosure Order, where any director, officer or Manager of the Service Provider or its Subcontractors (or any other Person having similar authority to the foregoing) authorizes, permits or acquiesces in the disclosure of Personal Information pursuant to a Disclosure Order;

(f) any storing, allowing access to, disclosure or use of Personal Information contrary to the provisions of *Freedom of Information and Protection of Privacy Act* (British Columbia) (without the prior written Approval of the Province as may be permitted under *Freedom of Information and Protection of Privacy Act* (British Columbia)); provided that, before the Province requires, in its sole discretion, that the occurrence thereof constitutes a "Material Breach" under this paragraph (f), the Province will have regard to all of the surrounding circumstances including, without limitation, the nature and significance of the breach, the compliance by the Service Provider and its Subcontractors (to the extent applicable) with the Province Policies and the Privacy Obligations, whether such breach is an isolated occurrence and the bearing thereof on the significance of the breach, and the steps and actions taken by the Service Provider (and its Subcontractors, to the extent applicable) to remedy or otherwise deal with the breach (including taking appropriate action against the Person or Persons involved) and the effectiveness and timeliness of such steps and actions

so taken, and whether or not the Personal Information in questions has been successfully recovered and whether it was used in any unauthorized way prior to such recovery (it being understood that such consideration will in no way prevent or prohibit the Province from determining that such breach constitutes a "Material Breach");

(g) failing to report the disclosure of Personal Information that is referred to under paragraph (f) above to the Province, provided that the Service Provider will not have committed a Material Breach of this Agreement pursuant to this paragraph (g) until such time as an individual who is a director, officer, Manager or in a Key Position is aware, or ought to have been aware, of such unauthorized access, disclosure or use of Personal Information, and has been provided with reasonable opportunity to report such unauthorized access, disclosure or use to the Province;

(h) taking action against an employee contrary to the provisions of Section 32 of **Schedule 24** *(Privacy Obligations)* which affords whistleblower protection to employees, provided that:

(i) where the Service Provider disputes that it has taken action against an employee contrary to **Schedule 24** *(Privacy Obligations)*, the Service Provider will not have committed a Material Breach of this Agreement as a result thereof until such matter is determined as between the Service Provider and the employee by an agreement in writing, or as a result of an arbitration or court proceeding, as the case may be, where all appeals with respect thereto have been exhausted, or the time to file an appeal has expired without a notice of appeal having been filed, as the case may be, and provided that the Service Provider is proceeding reasonably with respect to any dispute with such employee, and

(ii) in connection therewith, the Province will have regard to all of the surrounding circumstances leading up to any such actions taken by the Service Provider against the employee, including any use of the whistleblower protection provisions by such employee in order to prevent any disciplinary actions being taken by the Service Provider against such employee for other reasons;

(i) the occurrence of an Service Level Termination Event;

(j) any theft, fraud or other misappropriation of Province funds by the Service Provider, its Personnel or its Subcontractors or their External Personnel;

(k) any matter that is described in this Agreement as constituting a "Material Breach" for which no cure period is provided, and if a cure period is provided, then upon the failure of the Service Provider to rectify such breach within the applicable cure period therefor, or where such breach is not capable of being rectified within such cure period, then if the Service Provider fails to take or continue to take such steps and actions as may be necessary to rectify such breach, and in either case, to the satisfaction of the Province; or

(l) if the Service Provider breaches or defaults in the performance of any of its other material obligations under this Agreement or under any of the other Transaction Documents (other than a Service Level), which has an adverse effect upon the Province, and the Service Provider fails to rectify such breach within thirty (30) days (or such longer period as may be agreed to by the Province on a case-by-case basis) of its receipt of a written notice from the Province requesting it to do so, or where such breach is not capable of being rectified within thirty (30) days (or such longer period as may be agreed to by the

Province on a case-by-case basis), the Service Provider fails to take or continue to take such steps and actions as may be necessary to rectify such breach, and in either case, to the satisfaction of the Province.

28.2 Remedies of the Province.

Without the requirement for the Province to resort to the Dispute Resolution Process under Article 27 *(Dispute Resolution)* and without limiting any other rights or remedies that the Province may have at law, in equity, or as otherwise set forth in this Agreement, upon the occurrence of a Material Breach, the Province may invoke any one or more of the remedies set forth in **Schedule 37** *(Remedies for Material Breach)*.

28.3 Material Breach by Province.

The Province will be in material breach of its obligations under this Agreement (a "**Province Material Breach**") if the Province fails to pay when due, subject to Sections 15.5 (*Right of Set-Off*) and 15.6 (*Disputed Payments*), an amount in excess of $1,000,000.00 payable by the Province to the Service Provider pursuant to this Agreement that has not been subject to a Dispute (or an agreement between the Parties in settlement of a Dispute, whether through arbitration, mediation or otherwise), and the Province fails to rectify such failure within thirty (30) days of its receipt of a written notice from the Service Provider of such failure, such notice to state in detail the nature and specifics of the failure. The Service Provider may extend such thirty (30) day period, in its sole discretion, for such additional period of time upon written notice of such extension to the Province.

28.4 Remedies of the Service Provider.

Without the requirement for the Service Provider to resort to the dispute resolution process under Article 27 *(Dispute Resolution)* and without limiting any other rights or remedies that the Service Provider may have at law, in equity, or as otherwise set forth in this Agreement, upon the occurrence of Province Material Breach, the Service Provider may immediately terminate this Agreement by the delivery of a Termination Notice to the Province, in which case the provisions of Section 28.7 (*Termination Fees*) will apply.

28.5 Termination by Province for Convenience.

Notwithstanding any other provision contained in this Agreement, the Province may terminate this Agreement for convenience (for any reason or for no reason) on not less than 12 months prior written notice to the Service Provider at any time during the Term. For the purposes of this Section 28.5 (*Termination by the Province for Convenience*), the Termination Date will be the date stated in the Termination Notice.

28.6 Termination Notice.

Any Termination Notice from one Party to the other under this Agreement will specify the Termination Date, the grounds of termination (if applicable), the reasonable particulars of the surrounding circumstances giving rise to the grounds of termination, and if the Party providing the Termination Notice is the Province, whether any Termination Services will be required by the Province.

28.7 Termination Fees.

The responsibilities of the Parties for termination fees in connection with the Termination of this Agreement are set out in **Schedule 38** *(Termination Fees)*.

ARTICLE 29 – TERMINATION SERVICES

29.1 Termination Services.

During the Termination Assistance Period for each of the Data Centre Services and the Managed Services, as applicable, the Service Provider will provide the Province with the following services to facilitate the Province's repatriation of the Data Centre Services and/or the Managed Services, as applicable, or the orderly transition and migration thereof to an Alternative Service Provider, as the case may be, in an orderly, effective and efficient manner, and with minimal disruptions or adverse effect to the delivery of the applicable Services (collectively and in each case, the "**Termination Services**"):

(a) if the Province intends to consider the use of an Alternative Service Provider, upon the Province's request, assistance to the Province with respect to its describing the applicable Services that will be the subject of a competitive procurement process, bid specification or similar document in respect of the applicable Services provided that if the Parties do not enter into a Renewal Agreement for such Services, or if the Province does not provide the Service Provider with a notice of its intention to renew pursuant to Section 2.6 (*Renewal Notice*) in respect of such Services, then the Service Provider will provide the Province with the services referred to in this paragraph (a) immediately following a request therefor from the Province, notwithstanding that such request may be given by the Province earlier than the times referred to above in this Section 29.1 (*Termination Services*);

(b) cooperation with and assistance to the Province or the Alterative Service Provider in order to facilitate the transfer of the applicable Services to the Province or the Alternative Service Provider, as the case may be, in an orderly, effective and efficient manner and without any material interruptions or adverse effects to the Services so transferred;

(c) answers to all reasonable questions from the Province or the Alternative Service Provider regarding the applicable Services;

(d) copies of:

(i) the Documentation in electronic format, hard copy or both, as may be requested by the Province including, without limitation, a current listing and copies of all documented operational processes and procedures relating to the provision of the applicable Services as outlined in the Documentation, and

(ii) detailed lists and descriptions of all Data Centre Services or Managed Services, as applicable, which are then being provided (including volumes, Achieved Service Levels, up-to-date process maps, workflow charts, and other available policy and procedure documentation), technical information and technical descriptive documentation, and documentation of current configurations, to the extent not already included in the Documentation;

(e) subject to applicable privacy laws then in effect and to Section 29.7 (*Transfer of Personnel*), a current listing of all Personnel, and Subcontractors who are individual independent contractors (whether retained in their individual capacities or through corporate entities), who are performing the applicable Services ("**Available Personnel**"), a description of their roles and specific responsibilities in relation to the applicable Services, whether such Available Personnel are on leave or are active in performing the applicable Services, and their compensation and benefits entitlements;

(f) assistance with the transfer to the Province or the Alternative Service Provider of the Available Personnel in accordance with Section 29.7 (*Transfer of Personnel*);

(g) assistance with the provision of mutually agreed training for those Persons designated by the Province who will be assuming responsibility for the applicable Services following the Termination Date;

(h) copies of Subcontracts relating to the delivery of the applicable Services (whether or not expired with the Term of this Agreement), and provided that such Subcontracts were in use or otherwise in effect within three (3) years preceding the Termination Date;

(i) a general list of third person Software licensed and used by the Service Provider during the ordinary course of performing the applicable Services (the "**Termination Licensed Software**") on the Termination Date, and the Service Provider will, on the Termination Date or if the Service Provider requires the continued use of the Termination Licensed Software in order to perform the Termination Services, upon such date that the Service Provider no longer requires such use or otherwise on the Expiry of the Termination Assistance Period, whichever date is the later, assign and transfer, subject to **Schedule 43** (*Software Responsibility Table*) all rights and obligations of the Service Provider with respect to the Termination Licensed Software to the Province at no additional cost to the Province;

(j) a list of any Province Proprietary Software or Service Provider Software and all Modifications thereto used in providing the applicable Services, and copies of all Software and Modifications thereto which is being licensed to the Province in accordance with Article 19 (*Intellectual Property and Proprietary Rights*), or for which the license is being transferred to, or assumed by, the Province or the Alternative Service Provider, and all Source Code for such Software and Modifications for which the Service Provider has access, custody or control;

(k) detailed descriptions of the Systems used in the delivery of the applicable Services sufficient to permit the Province or the Alternative Service Provider to assume control of the provision of the applicable Services or to obtain and implement functional replacements therefor;

(l) assistance with appropriate testing of the Province's transition and migration procedures;

(m) assistance with respect to the transfer of relevant assets to the Province or the Alternative Service Provider in accordance with Section 29.6 (*Transfer of Assets, Contracts and Software*);

(n) the performance of the Service Provider's obligations under the Termination Assistance Plan;

(o) otherwise provide assistance and information requested by the Province in order to enable the smooth transition of the management of the applicable Services from the Service Provider to the Province or the Alternative Service Provider; and

(p) those matters referred to in Section 29.2 (*Termination Assistance Plan*), Section 29.6 (*Transfer of Assets, Contracts and Software*), Section 29.7 (*Transfer of Personnel*), and Section 29.10 (*Additional Termination Arrangements*).

The specific Termination Services to be provided by the Service Provider, including the Termination Services in respect of the foregoing, will be described more fully in the Termination Assistance Plan.

29.2 Termination Assistance Plan.

As part of the Termination Services, the Service Provider will develop and deliver a mutually agreed to termination assistance plan for the transition of the applicable Services from the Service Provider to the Province or to the Alternative Service Provider, as the case may be, in the manner set forth in this Article 29 (*Termination Services*) (the "**Termination Assistance Plan**"). For purposes thereof, the Service Provider will develop the framework for the Termination Assistance Plan within the first twenty-four (24) months following the Hand-Over Date. The framework for the Termination Assistance Plan will be reviewed by the Parties through the Governance Process on an annual basis. As part of the Termination Services, immediately upon the commencement of the Termination Assistance Period, the Service Provider will, in consultation with the Province and such other persons as the Province may direct, commence in good faith and with all reasonable diligence to develop the complete Termination Assistance Plan based upon the framework described above, and setting out in detail the specific tasks to be accomplished by each Party, and a schedule pursuant to which the tasks are to be completed. Such Termination Assistance Plan will, at a minimum, provide for the following:

(a) a communications plan for Personnel, Subcontractors and other interested parties;

(b) a plan relating to the making of offers of employment to the Available Personnel and the transitioning of employees who accept such offers of employment, and all related employee benefit arrangements in accordance with Section 29.7 (*Transfer of Personnel*);

(c) details of the reversion or transfer of the applicable Systems, the Personal Information, the Province Records, other Province Confidential Information, Province Proprietary Software and other materials and information to which the Province is entitled upon the termination or the expiry of this Agreement or the termination of the Data Centre Services or the Managed Services, as the case may be;

(d) a plan for the transfer of in-complete IM/IT projects, if any;

(e) a plan for the transfer of tangible personal property and the transfer or assignment of applicable contracts;

(f) support for Systems and Software testing to be carried out by the Province or the Alternative Service Provider in connection with the transfer or licensing of any Systems and Software;

(g) employee training;

(h) any modifications to the applicable Services to be provided during the Termination Assistance Period and the date or dates on which responsibility for the provision of the applicable Services or portions thereof are to be transferred to the Province or the Alternative Service Provider;

(i) any modifications to the Fees to take into account the planned reduction in Services and any increased or decreased costs associated with providing reduced Services over time that are agreed to in accordance with Section 29.3 *(Quality of Services)*;

(j) processes, methods and timelines in respect of the delivery of the Termination Services; and

(k) the anticipated conclusion date for the completion of the Termination Services;

The Parties will monitor the performance of the Termination Services and the Termination Assistance Plan on a regular basis through the Governance Process. The Parties agree to provide to each other reasonably sufficient information to create or update the Termination Assistance Plan as required in accordance with the terms of this Agreement. The Parties will revise and update the Termination Assistance Plan from time to time during the Termination Assistance Period.

29.3 Quality of Services.

The quality and level of performance of the Services by the Service Provider during the Termination Assistance Period will meet the applicable Service Levels then in effect. The Service Provider will not be required to meet the Service Levels with respect to any Services provided during that part of the Termination Assistance Period that occurs after Termination, except as may otherwise be agreed between the Parties through the Governance Process in the completion of the Termination Assistance Plan. The Service Provider will continue to provide the applicable Services during the Termination Assistance Period unless the Province expressly requests the permanent or temporary discontinuation thereof (or a portion thereof). Any permanent or temporary discontinuation of the applicable Services or any part thereof will be set out in the Termination Assistance Plan, or otherwise implemented through the Change Order Process.

29.4 Charges for Termination Services.

During the Term, the Service Provider will provide the Termination Services in the ordinary course of its delivery of the Services at no additional cost or charge to the Province, using all available Personnel and External Personnel. Any Termination Services delivered during the Term that have a material impact on the delivery and performance of the other Services will be deemed to be a Mandatory Change and will be addressed in the manner set forth in Article 7 (*Change Order Process*). After the Term, all Termination Services will be provided at the Standard Time and Materials Rates or Cost-Only Time and Materials Rates, as applicable, in accordance with a budget jointly prepared by the Parties and forming part of the Transition Assistance Plan and based upon the following:

(a) where the Termination is as a result of (i) the expiry of an applicable Initial Term or Renewal Term, as the case may be, (ii) Province Material Breach or (iii) Province Termination for Convenience, the Standard Time and Material Rates will apply; and

(b) where the Termination is as a result of the Material Breach of the Service Provider, the Cost-Only Time and Material Rates will apply.

29.5 Extension of Termination Services.

If the Province is unable to complete the transition of the applicable Services to the Province or the Alternative Service Provider, as the case may be, by the end of Termination Assistance Period, then upon not less than six (6) months prior written notice to the Service Provider, the Province may elect to extend the Termination Assistance Period for one (1) additional period of up to six (6) months beyond the then-effective date of the expiry of the Termination Assistance Period.

29.6 Transfer of Assets, Contracts and Software.

Upon Termination, for any reason, of this Agreement, the Data Centre Services or the Managed Services, as the case may be, and in connection with the transfer of the responsibility for the performance of the applicable Services to the Province or the Alternative Service Provider, as the case may be, the following provisions will apply:

(a) the Province or the Alternative Service Provider, as the case may be, will have the right (but not the obligation, unless specifically provided otherwise elsewhere in this Agreement) to purchase, or assume the lease of (as applicable), all applicable Dedicated Assets and applicable Designated Contracts (as they relate to the Data Centre Services or the Managed Services, as the case may be) from the Service Provider, and the Service Provider will, if such option is exercised, transfer, sell and assign the same to the Province or the Alternative Service Provider, as applicable, on the following terms:

(i) unless otherwise agreed in writing between the Parties or pursuant to the terms of the final Termination Assistance Plan, the effective date of transfer of such Dedicated Assets and Designated Contracts from the Service Provider to the Province or the Alternative Service Provider, as the case may be, will be on the Termination Date,

(ii) the Service Provider will be responsible, at its own cost and expense, for obtaining all necessary consents, approvals, authorizations, notices, requests and acknowledgements necessary to assign, transfer and convey such Designated Assets and Designated Contracts to the Province or the Service Provider hereunder, together with all applicable third party and Service Provider warranties associated therewith,

(iii) the purchase price for such Dedicated Assets owned (and not leased) by the Service Provider will be the fair market values of such assets, which the Parties agree will be an amount equal to the net book value of such Dedicated Assets on the books and records of the Service Provider, recorded in accordance with GAAP,

(iv) the Service Provider will sell such Dedicated Assets to the Province or the Alternative Service Provider on an "as-is" basis, free and clear of all Liens,

(v) notwithstanding the provisions of clause (iv) above, upon the exercise of the option to purchase such Dedicated Assets as contemplated under this paragraph (a), and prior to the selection of such Dedicated Assets by the Province or the Alternative Service Provider for transfer hereunder, the Service Provider will provide the Province with a written notice setting forth which, if any, of such Dedicated Assets are not in good working order, normal wear and tear excepted, or are not eligible (where applicable) for maintenance and support services without payment of additional fees or expenses other than ordinary ongoing maintenance and support charges,

(vi) in the case of Dedicated Assets leased by the Service Provider for which the Province or the Alternative Service Provider wishes to acquire the lease, the Service Provider will assign the lease of such Dedicated Assets to the Province or the Alternative Service Provider, on an "as-is" basis free and clear of all Liens

other than the interest of the lesser thereof, or such Liens as may have been granted therein by the lessor, and

(vii) any and all transfer and title fees, Taxes and charges in connection with the transfer of such Dedicated Assets under this Section will be borne by the Province;

(b) in respect of any Termination Licensed Software that is being used by the Service Provider to provide the applicable Services (other than off-the-shelf shrink wrap or clip wrap Software), at the option of the Province or the Alternative Service Provider, the Service Provider will transfer or assign the license for such Termination Licensed Software to the Province or the Alterative Service Provider, as the case may be, at no additional cost (other than the requirement for the Province or the Alternative Service Provider to pay ongoing license and maintenance fees, if applicable, in respect of such license);

(c) at the time that the Service Provider licenses any Termination Licensed Software (for use on a dedicated basis for use in providing the Services ((other than off-the-shelf shrink wrap or click wrap Software), the Service Provider will use reasonable efforts to obtain the right to transfer or assign the license upon Termination to the Province or the Alternative Service Provider in accordance with the provisions of paragraph (b) above at no additional charge to be paid to the licensor; and

(d) to facilitate the Province's or the Alternative Service Provider's acquisition of such Dedicated Assets, Designated Contracts and Termination Licensed Software, the Service Provider agrees (where commercially practical and subject to express provisions otherwise set forth in this Agreement) to acquire any material assets, Software and other rights in a manner that will enable the Service Provider to transfer the same to the Province or the Alternative Service Provider without the need to obtain and further consents upon the Termination of the Agreement. In the event that the Service Provider is not able to obtain such rights of transfer without having to obtain any further consents at the time of acquisition of any material assets, Software or rights, then the Service Provider will give the Province notice of the same prior to making such acquisition.

29.7 Transfer of Personnel.

Upon the Termination of this Agreement, and subject to Applicable Laws, the Province and the Alternative Service Provider will have the right to extend offers of employment to Available Personnel on such reasonable terms and conditions as the Province or the Alternative Service Provider, as the case may be, may determine. The Service Provider will provide access to such Available Personnel and will not interfere with the recruitment efforts of the Province or the Alternative Service Provider in respect of the Available Personnel.

29.8 Service Provider Severance Costs.

Except as expressly provided in Section 29.9 (*Province Severance Costs*), the Service Provider will be solely liable for any severance, termination or other payments which the Service Provider or an Affiliate of the Service Provider makes, or is required to make, to any of its employees or contractors who do or do not accept the offer of employment made by the Province or the Alternative Service Provider in accordance with Section 29.7 (*Transfer of Personnel*), or who do or do not receive an offer of employment from the Province or the Alternative Service Provider, as the case may be, upon Termination of this Agreement for any reason.

29.9 Province Severance Costs.

With respect to any non-executive Available Personnel of the Service Provider as of the Termination Date, and who do not receive offers of employment from the Province or the Alternative Service Provider (the "**Retained Employees**"), the Service Provider will have the right to seek reimbursement from the Province of the Severance Amount actually paid to any such Retained Employees in respect of the termination of their employment on a without cause basis, provided that:

(a) the Retained Employees are terminated on a without cause basis in connection with the Termination within thirty (30) days of the Termination Date;

(b) the Service Provider gives written notice to the Province requesting reimbursement not less than fifteen (15) days in advance of the intended date of termination of such Retained Employees, such notice to include the name of the Retained Employees whose employment will be terminated by the Service Provider, the proposed Severance Amount, the position and responsibilities of the Retained Employees, and the number of years of employment with the Service Provider (including any continued employment previously with the Province or its prior subcontractor);

(c) the Severance Amount is reviewed and Approved by the Province, acting reasonably and having regard to the requirements of any collective agreement governing the employment of such Retained Employees and Applicable Law;

(d) the Service Provider terminates the employment of such Retained Employees and pays the approved Severance Amount to such terminated Retained Employees within sixty (60) days of the Termination Date;

(e) the Service Provider provides evidence, as may be required by the Province, as to the termination of such Retained Employees and the payment of the approved Severance Amount to such terminated Retained Employees;

(f) to the extent that the Service Provider is entitled to require a release in connection with the payment of the Severance Amount, the Service Provider provides to the Province an originally signed release from such terminated Retained Employees releasing any and all liabilities and obligations of the Province to such terminated Retained Employees; and

(g) with respect to any Retained Employees who are providing the Termination Services to the Province under this Agreement, the dates set forth above in this Section 29.9 (*Province Severance Costs*) will be calculated from and after the last date on which the Termination Services are so provided by such Retained Employees to the Province hereunder, instead of from the Termination Date.

If the Province does not agree with or Approve the proposed Severance Amounts, then the Province will forthwith notify the Service Provider and the Service Provider will then consult with the Province and propose an alternate Severance Amount acceptable to the Province, acting reasonably. If the Parties are unable to agree upon the Severance Amount as between themselves for purposes of reimbursement under this Section 29.9 (*Province Severance Costs*), and regardless of any amount actually paid by the Service Provider to the terminated Retained Employees, then the matter will be a Dispute to be settled in accordance with the Dispute Resolution Process, and the provisions of Article 27 (*Dispute Resolution*) will survive the termination of this Agreement for purposes thereof. The Province will pay the Service Provider the Approved Severance Amount for the terminated Retained Employees pursuant to this Section

29.9 (*Province Severance Costs*) within thirty (30) days of the above conditions being satisfied, including the settlement of and Disputes pursuant to the Dispute Resolution Process.

29.10 Additional Termination Arrangements.

Without limiting the provisions of this Article 29 (*Termination Services*), if this Agreement is Terminated for any reason, then the Service Provider will, effective on the completion of the Termination Services or such other date as may be agreed to between the Parties or as otherwise contemplated in this Article 29 (*Termination Services*):

(a) peacefully leave and cause its Personnel and External Personnel to peacefully leave any Province facilities made available to the Service Provider in connection with providing the Services under this Agreement, and return to the Province and cause its Personnel and External Personnel to return all keys and access cards to such applicable facilities; and

(b) deliver to the Province all Documentation and other files, records and documents relating to the Services and all Province Confidential Information in whatever format, form, condition or media which are then in the possession or control of the Service Provider, or, at the request of the Province, destroy any Province Confidential Information and provide the Province with confirmation of the same.

29.11 Equitable Remedies of the Province.

The Service Provider acknowledges that the Province would suffer irreparable harm if the Service Provider breached (or attempted or threatened to breach) its obligations to provide Termination Services to the Province in accordance with and pursuant to the terms of this Agreement. In such event, the Province may proceed directly to a court of competent jurisdiction without having to exhaust or utilize the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*). If such court should find that the Service Provider has breached (or attempted or threatened to breach) any such obligations, then the Service Provider will not, without any additional findings of irreparable injury, harm or other conditions to injunctive relief, oppose the entry of an appropriate order compelling performance by the Service Provider and restraining the Service Provider from any further breaches (or attempted or threatened breaches) of its obligation to provide Termination Services hereunder.

29.12 Other Liabilities.

For greater clarification, in no event will the Province or the Alternative Service Provider assume or be liable for, and the Service Provider hereby agrees to indemnify the Province and any Alternative Service Provider from and against, any liabilities or obligations of the Service Provider not expressly assumed under this Agreement or in any other written agreement signed by the Province or the Alternative Service Provider, as the case may be.

ARTICLE 30 – FORCE MAJEURE AND LABOUR DISRUPTION

30.1 Notice of Force Majeure Event.

If either Party is prevented from, or delayed in performing any of its obligations under this Agreement as a result of a Force Majeure Event, or in anticipation of the occurrence of a Force Majeure Event, then the Party claiming the Force Majeure Event (or anticipation of the Force Majeure Event) will promptly notify the other Party by telephone (which does not include, for greater clarification, leaving a voice mail message). That Party will also provide the other Party with a follow up written notice within two (2) Business Days of such Party becoming aware of the potential non-performance or delay, of the particulars

of the Force Majeure Event (or anticipation of the Force Majeure Event) including details of the nature of the event, its expected duration and the obligations under the Agreement that will be affected by the Force Majeure Event (or anticipation of the Force Majeure Event). The Party claiming the Force Majeure Event (or anticipation of the Force Majeure Event) will continue to furnish reasonable reports with respect thereto to the other Party on a timely basis during the continuance of the Force Majeure Event. The notice requirements of this Section are in addition to any notices that may be required pursuant to Article 17 (*Business Continuity*).

30.2 Mitigation of Force Majeure Event.

Where a Party becomes aware of the occurrence of an event, condition or circumstance that could reasonably be expected to cause such Party to claim a Force Majeure Event, then that Party will use reasonable efforts to prevent or avoid such event, condition or circumstance developing into a Force Majeure Event, to the extent possible. Failing prevention of the occurrence of such Force Majeure Event by the use of such efforts, the Party claiming the Force Majeure Event will, during the continuance of such Force Majeure Event, use reasonable efforts to mitigate and minimize the effect of such Force Majeure Event, to reduce and minimize any ensuing delay or interruption in the performance of its obligations under this Agreement, and to recommence performance of its obligations under this Agreement whenever and to whatever extent possible and without delay. For greater clarification, where a Force Majeure Event affects performance of the obligations of both Parties under this Agreement, then both Parties may claim the same Force Majeure Event for purposes of this Article 30 (*Force Majeure and Labour Disruption*). Notwithstanding the foregoing, upon the occurrence or expected occurrence of a Force Majeure Event, the Service Provider will forthwith implement the Business Continuity Plan.

30.3 Application of Business Continuity Plan.

Upon the occurrence or expected occurrence of a Force Majeure Event the Service Provider will forthwith implement the Business Continuity Plan as contemplated in accordance with the terms thereof.

30.4 Consequences of Force Majeure Event.

Subject to the provisions of Section 30.3 (*Application of Business Continuity Plan*), during the occurrence of a Force Majeure Event, the obligations of the Party claiming the Force Majeure Event will be suspended, but only to the extent that such Party's obligations cannot be performed or are delayed as a result of the Force Majeure Event, and such Party will not be considered to be in breach or default under this Agreement for the period of such occurrence. The suspension of performance will be no greater in scope and of no longer duration than is reasonably required to adjust for effects of the Force Majeure Event, to the extent reasonably possible to do so. For greater clarification, no obligation of either Party that existed prior to the Force Majeure Event causing the suspension of performance will be excused as a result of the Force Majeure Event, unless such obligation is a continuing obligation, the performance of which is affected by the Force Majeure Event. During any Force Majeure Event, the Province may, in its discretion, exercise any one or more of the following remedies:

(a) during the period of time such Force Majeure Event remains in effect, not pay that portion of the Fees in respect of any Services so affected by the Force Majeure Event; and

(b) procure or otherwise obtain alternative services from any Person in replacement for or substitution of the affected Services during the period of time that the Force Majeure Event remains in effect, and for greater clarification, includes right of the Province to use the Fees so withheld from the Service Provider in accordance with paragraph (a) above to pay any such other Person for the alternative services.

30.5 Establishing a Force Majeure Event.

The Party claiming that a Force Majeure Event has occurred will bear the burden of proving the existence of such a Force Majeure Event and the consequences of such event.

30.6 Labour Disruption.

In the event of an occurrence or potential occurrence of a Labour Disruption preventing or delaying the performance of the obligations of the Service Provider under this Agreement, the Service Provider will:

(a) promptly notify Province by telephone of the particulars of the Labour Disruption including details of the nature of the Labour Disruption, its expected duration and the obligations of the Service Provider under this Agreement that will be affected by such Labour Disruption; and

(b) continue to furnish reasonable reports with respect to the status of the Labour Disruption to the Province on a timely basis during the continuance of the Labour Disruption.

In respect of the foregoing notice to the Province, the Service Provider may leave a voicemail message with the Province if necessary, but such voicemail message will not be deemed to be notice until actual voice contact is made, and the Service Provider will follow-up with written notice within three (3) Business Days of any verbal contact. Prior to claiming a Labour Disruption, the Service Provider will use its reasonable efforts to prevent or avoid the Labour Disruption, but not to the extent that the Service Provider would suffer substantial harm to its own commercial interests.

30.7 Effect of Labour Disruption.

A failure to provide any Services as a result of a Labour Disruption will not give rise to a Material Breach under this Agreement provided that the Service Provider continues to perform and provide the disrupted Services as soon as possible and continues to so use such efforts until the affected Services are restored.

30.8 Other Remedies.

During a Labour Disruption, the Province may, in its discretion, exercise any one or more of the following remedies in respect of the Services:

(a) not pay the Fees in respect of such other Services so affected (other than direct additional costs incurred by the Service Provider related to a partial delivery of such Services) during the period of time that the Labour Disruption remains in effect and such Services are disrupted or delayed; and

(b) procure or otherwise obtain alternative services from any Person in replacement for or substitution of the affected Services during the period of time that the Labour Disruption remains in effect and such Services are disrupted or delayed, and to off-set or deduct any costs thereof that are in excess of the Fees withheld pursuant to paragraph (a) above against any other Fees payable to the Service Provider under this Agreement.

30.9 Suspension of Maximum Credit Amount.

During the continuance of a Labour Disruption, the application of the Weightings for determining the Service Level Credits for those Services that are directly affected by the Labour Disruption will be suspended, such that the occurrence of the Labour Disruption will not adversely affect the requirement of

the Service Provider to pay the Service Level Credits in respect thereof, unless the Service Provider has failed to comply with this Article 30 (*Force Majeure and Labour Disruption*) including, without limitation, the requirement of the Service Provider to remedy the failure and to perform and provide the Services caused by the Labour Disruption.

ARTICLE 31 – ASSIGNMENT

31.1 Assignment by Province.

The Province may assign at any time, in its sole discretion, and without the Approval of the Service Provider but upon prior written notice, this Agreement in whole or in part, or sublicense any right or benefit set forth in this Agreement to any government, public sector or Crown entity, body or authority. Nothing in this Section will limit, or be deemed to limit, any rights granted in this Agreement with respect to Alternative Service Providers.

31.2 Assignment by Service Provider.

The Service Provider will not, either directly or indirectly, in whole or in part, assign this Agreement or any rights, duties, obligations or interests of the Service Provider under this Agreement, without the prior written consent of the Province, which consent may be given or withheld in the sole and absolute discretion of the Province. For the purpose of this Agreement, the following will be deemed to be an assignment:

(a) the amalgamation of the Service Provider or the Performance Guarantor with any other entity other than amalgamations with other Affiliates of the Service Provider that do not:

(i) cause a change in the Corporate Control of the Service Provider or the Performance Guarantor that would not be permitted under paragraph (d) below,

(ii) result in direct foreign ownership of any kind of the Service Provider, or

(iii) result in the Service Provider or the Performance Guarantor ceasing to be a Canadian Entity;

(b) an assignment by operation of law (but not including assignments by operation of law as a result of amalgamations permitted under paragraph (a) above);

(c) a sale of all or substantially all of the assets or undertaking of the Service Provider, the Performance Guarantor or the Corporate Guarantor;

(d) a direct change in the Corporate Control of the Service Provider or the Performance Guarantor, other than a direct change in Corporate Control of the Performance Guarantor in circumstances where:

(i) the Performance Guarantor:

(A) continues to be a Canadian Entity; and

(B) continues to be under the Corporate Control of an Affiliate of the Corporate Guarantor, and

(ii) any such change in Corporate Control does not adversely impact or otherwise adversely affect the Performance Guarantee or the Corporate Guarantee, as determined by the Province in its discretion; or

(e) any direct foreign ownership of any kind of the Service Provider.

Any attempt by the Service Provider to so assign all or any part of this Agreement or any of the Service Provider's rights, duties, obligations or interests under this Agreement, without the prior written consent of the Province, will be null and void and without effect, and will constitute a Material Breach of this Agreement under Subsection 28.1(k) (*Service Provider Material Breach*), giving rise to the right of the Province to terminate this Agreement. For greater clarification, at no time will the Province consent to any assignment where such assignment could in any manner expose any Personal Information to any increased risk of access, use or disclosure contrary to the terms of this Agreement. Notwithstanding the foregoing, the Subcontracting by the Service Provider of any of its rights, duties, obligations or interests under this Agreement in accordance with the provisions of Article 12 (*Subcontractors*) will not constitute or be deemed to constitute an assignment under this Section 31.2 (*Assignment by Service Provider*).

ARTICLE 32 – CONTRACTUAL RELATIONSHIP

32.1 Relationship of the Parties.

Except as otherwise set forth in this Agreement:

(a) nothing in this Agreement will be construed to grant the Service Provider any right to act as an agent for or on behalf of the Province, including with respect to the Stakeholders, the Clients, third parties or any other Person; and

(b) the Service Provider has no authority to bind, and will not bind or purport to bind, the Province with respect to any such Stakeholders, Clients, third parties or any other Person with respect to the performance of the Services or any matter relating to the Services, without the express Approval of the Province.

For greater clarification, the use by the Service Provider of the Province Marks in performing the Services under this Agreement, and the assumption by the Service Provider or its Affiliates of any Assigned Contracts, will not be, or be deemed to be, an act of the Service Provider (or its Affiliates, as applicable) as agent for and on behalf of the Province, and in all such cases the Service Provider (or its Affiliates, as applicable) will be, and will be deemed to be, acting on its own behalf, in its own right and as a independent contractor. The Service Provider expressly agrees not to act or to purport to act as agent for and on behalf of the Province, and not to bind or to purport to bind the Province, unless authorized to do so by express and prior Approval of the Province.

32.2 No Partnership or Joint Venture.

This Agreement establishes, and will only be construed as establishing, a contract between unrelated business entities for the provision of certain services, and does not and will not be construed or deemed to create or constitute a partnership or joint venture relationship between the Parties. Each Party hereby expressly disclaims any intention to create a partnership or a joint venture with respect to the subject matter of this Agreement. Each Party will be independently and solely responsible for all obligations arising in connection with its own employees (including any obligations incumbent upon such Party as an employer, such as the payment of benefits, and the withholding and remittance of applicable source deductions, in respect of its employees).

32.3 Conflict of Interest.

At no time during the Term will the Service Provider or its Personnel directly or indirectly engage in any activity, business or undertaking that could create a conflict of interest or perceived conflict of interest with the Province in respect of all or any part of the Services (it being acknowledged by the Parties that the different economic interests of the Parties in and of itself will not be deemed to be a conflict of interest under this Section). In connection therewith, the following provisions will apply:

(a) where the Service Provider becomes aware of any act, omission or event that could be construed as creating a conflict of interest or a perceived conflict of interest in respect of all or any part of the Services, or where the Service Provider is uncertain as to whether or not a conflict of interest or a perceived conflict of interest could exist in a particular situation, the Service Provider will immediately notify the Province of the same;

(b) the Service Provider will abide by any direction given by the Province in respect of any such act, omission or event, except where the Service Provider reasonably disagrees with such direction from the Province, in which case such matter will be deemed to be a Dispute and will be resolved in accordance with the Dispute Resolution Process;

(c) if such Dispute is settled by arbitration, then the Dispute will be determined by the arbitrator (or arbitrators) in accordance with any Province Policies or processes demonstrably utilized or held by the Province in respect of conflicts of interest;

(d) the Province retains the right to prohibit any Person (including any Subcontractor or Supplier to of the Service Provider) from taking any action, delivering any Services or otherwise participating in any manner with respect to the Services or to this Agreement where the Province determines, in its sole opinion, that such Person's current or past corporate or other interests may give rise to a conflict of interest in connection therewith; and

(e) any determination or direction by the Province in respect of paragraph (d) above will be based upon such information as the Province, in its sole discretion, determines to be relevant.

32.4 Code of Conduct and Standards.

The Service Provider will at all times comply, and will cause its Personnel to comply, with the Service Provider code of conduct policy, a copy of which is attached to this Agreement as **Schedule 39** *(Service Provider Code of Conduct)*, as such policy is revised from time to time upon written notice to the Province. The Service Provider will also require its Personnel to conduct themselves in a manner consistent with the "conflicts of interests" guidelines as set forth in the *Standards of Conduct for Public Services Employees* (British Columbia), a copy of which has been provided by the Province to the Service Provider, as such standard is revised by the Province from time to time upon notice to the Service Provider (but excepting out compliance with any such revised standards that could reasonably result in adverse labour relations between the Service Provider and those of its Personnel who are governed by a collective agreement then in force). Should there be a conflict or inconsistency between the Service Provider code of conduct policy and the Province's the *Standards of Conduct for Public Services Employees* (revised from time to time as previously provided), then the higher or more stringent code of conduct, policy or standard will govern.

32.5 Province's Conflict of Interest Policy.

The Service Provider represents, warrants and covenants that none of its members or employees has given, and nor will they give, any commissions, payments, kickbacks, lavish or excessive entertainment, or other inducements of more than minimal value in any form to any employee or agent of the Province in connection with this Agreement. The Service Provider acknowledges that the giving of any such inducements or gifts is strictly in violation of the Province's policy on conflicts of interest, and may result in cancellation of this Agreement and all future contracts between the Parties. The Service Provider acknowledges that it has read the Province's policy on conflicts of interest, and it agrees that it will abide by such policy during the Term, as such policy is revised from time to time upon reasonable notice to the Service Provider.

ARTICLE 33 – MISCELLANEOUS

33.1 Notice.

Unless specifically provided otherwise in this Agreement, including through the Governance Process, wherever any notice, communication, demand, invoice, Approval or other document is required or permitted to be given, sent or delivered by one Party to another under this Agreement, then it will be in writing and may be delivered personally, by facsimile or sent by a recognized courier service (and for greater clarification, no notice, demand or Approval required or permitted to be given under this Agreement will be, or be deemed to be, effective or delivered if given by email). Any such notice, communication, demand, invoice, Approval or other document so personally delivered or sent by facsimile or courier will be deemed to be given when actually received and will be addressed as follows:

To the Province:

The Province of British Columbia
4000 Seymour Place
Victoria, British Columbia
V8W 9V1

Attn: Executive Director, Enterprise Hosting Solutions, Workplace Technology Services
Fax: (250) 387-2907

To the Service Provider:

EDS Advanced Solutions
Suite 2200 – 4464 Markham Street
Victoria, British Columbia
V8Z 7X8

Attn: President
Fax: (250) 405-4522

Either Party may change its address or facsimile number for notices upon giving prior written notice of the change to the other Party in the manner provided above.

33.2 Appropriation and Approvals.

Notwithstanding any other provision of this Agreement, the payment of money by the Province to the Service Provider under this Agreement is subject to:

(a) there being sufficient monies available in an appropriation, as defined in the *Financial Administration Act* (British Columbia), to enable the Province to make that payment; and

(b) Treasury Board, as defined in the *Financial Administration Act* (British Columbia), not having controlled or limited, under the *Financial Administration Act* (British Columbia), expenditure under any appropriation referred to in paragraph (a) above.

33.3 Severability.

If any provision contained in this Agreement or its application to any Person or circumstance will, to any extent, be invalid or unenforceable, then the remainder of this Agreement or the application of such provision to Persons or circumstances other than those to which it is held invalid or unenforceable, will not be affected, and each provision of this Agreement will be separately valid and enforceable to the fullest extent permitted by law. In addition, any provision of this Agreement which is prohibited or unenforceable in any jurisdiction will not invalidate the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction will not invalidate or render unenforceable such provision in any other jurisdiction. In respect of any provision determined to be unenforceable or invalid in a court having competent jurisdiction, the Parties agree to negotiate in good faith to replace the unenforceable or invalid provision with a new provision that is enforceable and valid in order to give effect to the business intent of the original provision to the extent permitted by Applicable Law, and in accordance with the intent of this Agreement. For greater clarification, if the application of any provision of this Agreement, either generally or in a particular situation, would require a Party to act in a manner contrary to Applicable Law, then such provision will be deemed to be stricken from this Agreement (either generally or in such particular situation, as appropriate), and the affected Party will not be in breach of the Agreement or liable for damages for complying with such Applicable Law.

33.4 Entire Agreement.

This Agreement and the Schedules to this Agreement, together with the other Transaction Documents, and all other documents or agreements referred to in this Agreement, the Schedules and the other Transaction Documents, constitute the entire agreement among the Parties with respect to the subject matter hereof, and cancel and supersede any other prior agreements, undertakings, declarations, commitments, representations, warranties, conditions, promises and understandings, whether written or oral, express or implied, statutory or otherwise among the Parties with respect to the subject matter of this Agreement.

33.5 Amendments.

No term or provision of this Agreement may be amended except by written instrument signed by each of the Parties, by a Change Order as contemplated in Article 7 (*Change Order Process*), or by a unilateral notice of declaration given or made by one Party pursuant to the terms of this Agreement, in respect of a change or amendment that such Party is entitled to make under the terms of this Agreement without the requirement for the Approval of the other Party, if any.

33.6 No Liens or Charges against Provincial Assets.

Except as expressly provided in this Agreement, the Service Provider covenants and agrees to protect and keep free of all assets used in the provision of the Services and assets of the Province from any and all Liens, other than interests of a lessor in any leased assets or Liens granted by any lessor in such leased assets. If any such Lien is filed, then the Service Provider will immediately notify the Province by providing a copy of the Lien claim, and will cause such Lien to be satisfied or otherwise discharged within ten (10) Business Days. If any such Lien is filed or otherwise imposed, and the Service Provider

does not cause such Lien to be released and discharged forthwith, then the Province has the right, but not the obligation, to pay all sums necessary to obtain such release and discharge, or otherwise cause the Lien to be removed to the satisfaction of the Province, from funds retained from payment then due or thereafter to become due as Fees payable to the Service Provider under this Agreement.

33.7 Waiver.

Failure by a Party to insist in any one or more instances upon the strict performance of any one of the terms, provisions or covenants contained in this Agreement will not be construed as a waiver or relinquishment of such term, provision or covenant. No consent or waiver, express or implied, by a Party to or of any breach or default by another Party in the performance by such other Party of any term, provision or covenant under this Agreement will be deemed or construed to be a consent or waiver to or of any other breach or default such other Party under this Agreement. No waiver of any breach of any term, provision or covenant of this Agreement will be effective or binding unless made in writing and signed by the waiving Party.

33.8 Further Assurances.

Each of the Parties will, from time to time, execute and deliver all such further documents and instruments and do all such further acts and things as the other Party may reasonably require to carry out or better evidence or perfect the full intent and meaning of this Agreement.

33.9 Obligations as Covenants.

Each obligation of a Party in this Agreement, even though not expressed as a covenant, is considered for all purposes to be a covenant.

33.10 Transaction Fees.

Each Party will be responsible for and pay its respective legal and accounting costs and other expenses incurred in connection with the preparation, execution and delivery of this Agreement (including all prior steps and actions taken in respect to the JSRFP), the other Transaction Documents and all other documents and instruments prepared, executed or delivered pursuant thereto or to this Agreement.

33.11 Survival.

Unless otherwise provided in this Agreement, the following provisions, including the obligations of the Service Provider and the Province thereunder will survive the expiration or termination of this Agreement:

- Section 1.4 (*Interpretation*);
- Section 1.5 (*Acting Reasonably*);
- Section 2.11 (*Termination Assistance*);
- Section 2.12 (*Effect of Termination*);
- Section 3.10 (*Effect of Termination Prior to Hand-Over Date*);
- Section 10.1 (*Use of Province Marks*);
- Section 10.4 (*Publicity*);
- Section 12.1 (*Responsibility for Subcontractors*);

- Section 14.1 (*Maintenance of Records*)
- Section 14.3 (*Custody of Province Records*);
- Section 14.4 (*Control of Province Records*)
- Section 14.5 (*Final Return of Province Records*);
- Section 14.7 (*Storage and Disposal of Records*);
- Section 14.8 (*Locations of Records*);
- Article 15 (*Fees and Payment Terms*);
- Section 16.2 (*Foreign Discourse*);
- Section 16.6 (*Safeguarding Confidential Information*);
- Section 16.7 (*Permitted Disclosures and Use of Confidential Information*);
- Section 16.8 (*Province Permitted Disclosure*);
- Section 16.9 (*Exceptions to Obligations of Confidentiality*);
- Section 16.10 (*Disclosures Compelled by Law*);
- Section 16.11 (*Disclosure of Personal Information*);
- Section 16.12 (*Court Order Disclosure*);
- Section 16.13 (*Notification of Unauthorized Use of Confidential Information*);
- Section 16.14 (*Breach of Confidentiality*);
- Section 16.15 (*No Rights to Confidential Information*
- Section 19.1 (*Ownership of Province Assets*);
- Section 19.2 (*Ownership of Province Proprietary Software*);
- Section 19.5 (*Assignment of Intellectual Property*);
- Section 19.6 (*Service Provider Personnel, Subcontractors and External Personnel*);
- Section 19.10 (*License to Use SP Proprietary Software*);
- Section 19.17 (*Use of Confidential Information in License Rights*);
- Section 20.13 (*Termination of Rights to Province Shared Infrastructure*);
- in respect of an audit conducted by the Province of the last Contract Year, Section 22.1 (*Access Rights*), Section 22.2(*Examination and Copies*), Section 22.4 (*Audit Rights*), Section 22.5 (*Costs*, and Section 22.7 (*General Principles*);
- Section 23.3 (*FOIPPA Inspections*);
- Article 25 (*Indemnification, Liability and Guarantees*);
- Article 27 (*Dispute Resolution*);
- Section 28.7 (*Termination Fees*);
- Article 29 (*Termination Services*);
- Section 31.2 (*Assignment by Service Provider*);

- Section 33.11 (*Survival*);
- Schedule 23 (*Fees*);
- the Performance Guarantee and the Corporate Guarantee; and
- any other provisions of this Agreement which are required for the proper interpretation thereof.

In addition, any liabilities or obligations of either Party arising before Termination of this Agreement or arising out of the events causing such Termination, and any damages or other remedies to which a Party may be entitled under this Agreement, whether at law or in equity, arising from any breach of such obligations of a Party and any other provisions herein, the nature and intent of which is to survive Termination of this Agreement, will survive and will not be affected by the expiration or Termination of this Agreement.

33.12 Language.

The Parties have agreed that this Agreement and all documents related to this Agreement will be drafted in the English language. Les parties aux présentes ont convenu que cette convention et tous les documents qui s'y rapportent soient rédigés en langue anglaise.

33.13 Governing Law.

(a) This Agreement will be governed by and construed in accordance with the laws, other than choice of law rules, of the Province of British Columbia. Any matter regarding the interpretation and application of this Agreement or the other Transaction Documents, and all disputes arising under or in connection with this Agreement or the other Transaction Documents will, subject to Article 27 (*Dispute Resolution*), be within the exclusive jurisdiction of the courts of British Columbia, as stipulated in the following paragraph.

(b) Subject to Article 27 (*Dispute Resolution*), the Parties irrevocably agree to and hereby accept and attorn to the exclusive jurisdiction of the Courts of British Columbia for any and all Claims that they may have related in any way to this Agreement and its renewal or non-renewal, and all Disputes relating hereto or hereunder, and the Parties irrevocably covenant and agree not to commence any action or bring any Claim in any forum whatsoever, be it domestic, foreign or international (including, but not limited to the *North American Free Trade Agreement*), relating in any way to this Agreement or its renewal or non-renewal or any Dispute relating hereto or hereunder.

(c) The Parties further agree that, should any third party initiate any action under any of the dispute settlement provisions of the *World Trade Organization Agreement* or the *North American Free Trade Agreement* (including but not limited to Chapter Eleven thereof), in any way relating to this Agreement, then no Party will provide any assistance whatsoever (including, without limitation, financial assistance, access to documents and access to personnel) to such third party to pursue any such action. The Parties will also provide all reasonable assistance, one to the other, to defend against such third party claims.

(d) The Service Provider, on its own behalf and on behalf of all others who may claim through it or under it, including but not limited to the Performance Guarantor and the Corporate Guarantor and their respective Affiliates (collectively, the "**Service Provider Group**") hereby covenants and agrees that, without the express written consent of the Province (which may be withheld for any cause, or without cause), none of the Service Provider Group will make any Claim or take any proceedings whatsoever concerned or

related to any matter arising under or relating to this Agreement against any Person under Chapter Eleven of *the North American Free Trade Agreement.*

(e) The Service Provider, on its own behalf and on behalf of the Service Provider Group, hereby specifically acknowledges that the provisions of this Section 33.13 (*Governing Law*) are fundamental to this Agreement. The Province has fundamentally relied upon the presence of all of these provisions and the Province would not have entered into this Agreement with the Service Provider without these provisions being included.

33.14 Change of Law.

The Service Provider hereby acknowledges and agrees that its costs involved in performing its obligations under this Agreement are, in part, based upon governmental laws, regulations and policies in force at the time this Agreement was entered into and subsequently, and that such governmental laws, regulations and policies are subject to change without notice. Any such change could result in a material change in the Service Provider's costs of performing its obligations under this Agreement. The Service Provider specifically acknowledges and agrees that:

(a) any such change that has the effect of increasing the Service Provider's costs of performing its obligations under this Agreement will not effect those obligations;

(b) such actions will not constitute expropriation or be tantamount to expropriation at domestic or international law (including, but not limited, the *North American Free Trade Agreement*); and

(c) such actions will not constitute grounds for asserting any other claim whatsoever under domestic law or any claim whatsoever under any international agreement (including, but not limited to, Chapter Eleven of the *North American Free Trade Agreement* and the *General Agreement on Trade in Services*).

33.15 No Fettering of Legislative Authority.

The Service Provider expressly acknowledges and agrees that nothing in this Agreement will be construed as an agreement by the Province to restrict, limit or otherwise fetter in any manner the Province's ability to introduce, pass, amend, modify, replace, revoke or otherwise exercise any rights or authority regarding legislation, regulations, policies or any other authority of the Province.

33.16 Procurement.

The Parties hereby acknowledge and affirm that this Agreement constitutes a "procurement" by the Province as that term is utilized in the *North American Free Trade Agreement* and the *General Agreement on Trade in Services*, and consequently:

(a) *North American Free Trade Agreement* Articles 1102, 1103, 1107, 1106(1)(b), (c), (f), and (g), and 1106(3)(a) and (b) do not apply to this Agreement, by virtue of the *North American Free Trade Agreement* Articles 1108(7)(a) and 1108(8) (b);

(b) *North American Free Trade Agreement* Chapter Twelve does not apply to this Agreement by virtue of Article 1201(2)(c);

(c) the Services being procured under this Agreement are services supplied in the exercise of governmental authority for purposes of the *General Agreement on Trade in Services*; and

(d) Articles II, XVI and XVII of the *General Agreement on Trade in Services* do not apply to this Agreement because, for purposes of Article XIII of that agreement, this Agreement constitutes a procurement by a governmental agency of services being purchased for governmental purposes and not with a view to commercial resale or with a view to use in the supply of services for commercial sale.

33.17 Binding Effect.

This Agreement will be binding upon and enure to the benefit of the Parties and their respective successors and permitted assigns.

33.18 No Third-Party Beneficiaries.

Nothing in this Agreement, express or implied, is intended to confer upon any Person (other than the Parties and their successors and permitted assigns), and the indemnified parties who are expressly indemnified pursuant to the provisions of this Agreement, any rights, benefits or remedies of any kind or character whatsoever, and no Person will otherwise be deemed to be a third-party beneficiary under or by reason of this Agreement, unless specifically provided otherwise in this Agreement.

33.19 Counterparts.

This Agreement may be executed in several counterparts, each of which will be deemed to be an original. Such counterparts together will constitute one and the same instrument, notwithstanding that all of the Parties are not signatories to the original or the same counterpart.

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, AS REPRESENTED BY THE MINISTER OF LABOUR AND CITIZENS' SERVICES:

L Wanamaker

Name: Lori Wanamaker
Title: Deputy Minister, Ministry of Labour and Citizens' Services

EDS ADVANCED SOLUTIONS INC.

(c/s)

By: _____
Name: Al Hurd
Title: Chair

SCHEDULE 2

TRANSITION PLAN

See attached.

SCHEDULE 2 – TRANSITION PLAN

Table of Contents

V0.8.2 STMS Schedule 2 - Transition Plan

ID	Task Name	Start	Duration	Finish	Pred	Resource Names
1	**V0.8.1_STMS Schedule 2 - Transition Plan**	**Mon 01 Sep '08**	**195 days**	**Fri 29 May '09**		
2						
3	**Hand-Over Date**	Mon 30 Mar '09	0 days	Mon 30 Mar '09		
4	**Human Resource Activities**	**Mon 01 Sep '08**	**195 days**	**Fri 29 May '09**		
5	Preliminary Information Gathering	Mon 01 Sep '08	22 days	Tue 30 Sep '08		SP
6	Prepare and distribute Offer Letters (Oct 17th & Nov 4/08)	Fri 05 Sep '08	43 days	Tue 04 Nov '08		SP
7	Legal Review and Approval of Union Contract Consolidation	Thu 02 Oct '08	22 days	Fri 31 Oct '08		SP
8	Consolidation of Collective Agreements	Fri 05 Sep '08	45 days	Thu 06 Nov '08		SP
9	Union Consultation on Process & Transition	Fri 05 Sep '08	41.7 days	Mon 30 Mar '09		SP
10	Address Security and Criminal Record Checks	Mon 01 Sep '08	60.25 days	Mon 30 Mar '09		SP
11	Detailed Information Gathering (detailed employee personal & payroll data)	Wed 19 Nov '08	20 days	Fri 09 Jan '09		SP
12	Address Pension Issues	Fri 05 Sep '08	26 days	Fri 10 Oct '08		SP
13	Address Benefit Issues	Fri 05 Sep '08	71 days	Fri 12 Dec '08		SP
14	Secure WHS Position Approvals from SP/HP	Wed 01 Oct '08	53 days	Fri 12 Dec '08		SP
15	Payroll Set up and verification	Mon 12 Jan '09	27.35 days	Mon 30 Mar '09	11,6	SP
16	**Employee Communications**	**Wed 08 Oct '08**	**124 days**	**Mon 30 Mar '09**		**SP**
17	Townhalls	Wed 08 Oct '08	124 days	Mon 30 Mar '09		SP
18	**One on One's**	**Fri 31 Oct '08**	**1 day**	**Fri 31 Oct '08**		
19	One on One's	Fri 31 Oct '08	1 day	Fri 31 Oct '08		SP
20	**Orientation & Acclimation**	**Fri 27 Mar '09**	**0 days**	**Fri 27 Mar '09**		
21	Orientation & Acclimation Begins	Fri 27 Mar '09	0 days	Fri 27 Mar '09		SP
22	Knowledge Transfer	Mon 03 Nov '08	107 days	Fri 29 May '09		SP
23	Staff Augmentation	Wed 19 Nov '08	94 days	Fri 29 May '09		SP
24	Staffing	Thu 02 Oct '08	125 days	Fri 29 May '09		SP
25	**Security Activities**	**Tue 30 Sep '08**	**1 day**	**Tue 30 Sep '08**		
26	Policy Gap Analysis (ESIS to Core Policy & ISP)	Tue 30 Sep '08	1 day	Tue 30 Sep '08		SP
27	**Service Management Activities**	**Mon 02 Feb '09**	**42 days**	**Tue 31 Mar '09**		
28	Review of Province Operating Manuals	Mon 02 Feb '09	35 days	Fri 20 Mar '09		SP
29	Supervise review of Province Operating Manuals	Mon 02 Feb '09	35 days	Fri 20 Mar '09	28SS	Prov
30	Province will provide complete & accurate inventory for hardware & software	Mon 30 Mar '09	2 days	Tue 31 Mar '09	3	Prov
31	Province will provide authorization matrices and contact info	Mon 30 Mar '09	2 days	Tue 31 Mar '09	3	Prov
32	**Service Provider Business Operations Implementation**	**Fri 05 Sep '08**	**186 days**	**Fri 22 May '09**		

ID	Task Name	Start	Duration	Finish	Pred	Resource Names
33	Develop Project Milestone Schedule	Fri 05 Sep '08	61 days	Fri 28 Nov '08		SP
34	Implement Project Issues/Risk Management Process (DAIR & 4 Up Report) -	Fri 05 Sep '08	67 days	Mon 08 Dec '08		SP
35	Establish Status Reporting	Fri 14 Nov '08	1 day	Fri 14 Nov '08		SP
36	Identify Work-In-Progress Projects	Fri 14 Nov '08	57 days	Mon 02 Feb '09		Prov
37	Update Transformation Progam to support assumption of Work-In-Progress Projects	Mon 30 Mar '09	40 days	Fri 22 May '09	3	SP
38	**Facilities Activities**	**Fri 05 Sep '08**	**147 days**	**Mon 30 Mar '09**		
39	Q9 Data Centre Site Selection	Wed 01 Oct '08	89 days	Mon 30 Mar '09		SP
40	Arrangements completed for lease of office facilities	Fri 05 Sep '08	147 days	Mon 30 Mar '09		SP
41	**Sub-Contractor Agreements**	**Fri 05 Sep '08**	**146.25 days**	**Mon 30 Mar '09**		
42	Complete subcontract with Q9 Networks Inc	Fri 05 Sep '08	117 days	Mon 30 Mar '09		SP
43	Complete subcontract with Myra Systems Corp.	Fri 05 Sep '08	117 days	Mon 30 Mar '09		SP
44	Complete subcontract with EMC Corporation of Canada	Fri 05 Sep '08	117 days	Mon 30 Mar '09		SP
45	Complete subcontract with Sun Microsystems Canada	Fri 05 Sep '08	117 days	Mon 30 Mar '09		SP
46	**Receive Transferred Records from Province (Owner = TBD)**	**Fri 28 Nov '08**	**87 days**	**Mon 30 Mar '09**		
47	Province will provide records to SP	Fri 28 Nov '08	87 days	Mon 30 Mar '09		Prov

SCHEDULE 3 – TRANSITION MANAGEMENT AND GOVERNANCE

Table of Contents

1. SUMMARY AND SCOPE OF SERVICES

1.1 Definitions

Capitalized words used in this Schedule shall incorporate the meanings given to such words in the Agreement. In the event that a term is not defined in the Agreement, it shall have the meaning provided in Appendix A *(Definitions)* of this Schedule or in the body of this Schedule.

1.2 Purpose of this Document

1.2.1 General

This Schedule describes the scope of the Transition Management and Governance activities to be performed by the Parties under the Agreement and the responsibilities of the Parties in connection therewith.

This Transition Management and Governance Schedule must be read in conjunction with the Transition Plan attached as Schedule 2 *(Transition Plan)* to the Agreement. The Transition Plan sets forth the detailed schedule of tasks to be performed to accomplish the Transition activities documented in this Schedule.

1.2.2 Appendices

The following Appendix is attached and forms part of this Schedule, whether or not it is specifically referred to in this Schedule:

Appendix A – Definitions

1.3 Related SOWs and Schedules

The Parties acknowledge and agree that this Schedule is subject to the provisions of the Agreement and Schedules to the Agreement; however, the Parties have identified the following SOWs or Schedules to the Agreement as being important to the understanding of Services set forth in this Schedule:

Schedule 2 – Transition Plan
Schedule 4 – Work-in-Progress Projects
NTD: not aware if anyone is assigned to write Schedule 4. Deb Buckle has a list of the Work-in-Progress Projects that was formerly included as an Appendix of Schedule 2
Schedule 9 - Transformation
Schedule 10 – Transformation Plan

2. Transition Scope

This Transition Schedule sets out specific tasks and deliverables that are required for the Transition referenced in Section 3.2 *(Hand-Over of Services)* of the Agreement. This document is the supporting narrative in respect to a detailed plan which is set out in Schedule 2 *(Transition Plan)* to the Agreement.

2.1. Management and Governance

With respect to those activities described in this Schedule that are completed after the Hand-Over Date, the Parties will utilize the Transition Governance Process described in the Agreement.

The Service Provider has appointed a Transition project manager who, on behalf of the Service Provider, is responsible for reporting, engaging escalation processes and who will act as the liaison to the to the Province for all Transition activities.

The Province has appointed a Transition project manager who, on behalf of the Province, is responsible for reporting, escalation processes and who will act as the liaison to the Service Provider for all Transition activities.

2.1.1. Transition Management Team

The composition of the Transition Management Team of the Province and the Service Provider is set out below. During the Transition Period, being the period of time commencing on the Hand-Over Date and ending one month thereafter, the members of the Transition Management Team will be dedicated primarily to the implementation of the Transition.

The Transition Management Teams will conduct joint reviews on a regular basis in order to monitor the progress of the Transition and to identify issues that may affect the schedule for completion of the Transition activities. Any potential delays or circumstances that may adversely affect the Transition will be escalated in accordance with the Transition Governance Process.

Team Focus	Province Lead	SERVICE PROVIDER Lead
Transition Management	Deborah Buckle	
Human Resources	Jody Weeks	
Mainframe	Kim Jordheim	
Midrange	Michael Hayes	
Storage and Backup	Lee Johnson	
Data Centre	Dave Dube	
Network LAN/WAN	Brian Severinson	
Disaster Recovery and	Dave Dube	

At issue for Inquiry

Team Focus	Province Lead	SERVICE PROVIDER Lead
Business Continuity Planning		
Security	Dave Campbell	
Service Management	Rose Justice	
Transformation	Deborah Buckle	
Privacy	Sharon Plater	
Service Level Agreements	Brad Kocurek	
Service Provider Business Operations	Not Applicable	At issue for Inquiry
Service Provider Facilities	Not Applicable	
Service Provider Sub-Contractor Agreements	Not Applicable	
Receive Transferred Records from the Province	Brad Kocurek	

3. Human Resources Activities

The activities with respect to the Transition that relate to Human Resources include the following that will be undertaken prior to, during and following the Hand-Over Date:

(i) Engaging in discussions and negotiations with the BCGEU.
(ii) Preparing offers to Province employees and other prospective employees.
(iii) Preliminary gathering of necessary information from new employees.
(iv) Arranging for and holding open house sessions for employees who are new to their positions.
(v) Holding orientation and training sessions for employees who are new to their positions.
(vi) Establishing SAP payroll recording for new employees.

3.1 Milestones Completed by Hand-Over Date – Human Resources Activities

The following activities have been completed by the Hand-Over Date:

(i) Agreement with BCGEU for the transfer of Province employees to Service Provider.
(ii) Agreement regarding the scope of and process for Criminal record checks ("CRC"s).
(iii) Preparation and distribution of letters offering employment to Province employees.
(iv) Establishment of pension and benefits plans.
(v) Town halls and communication with employees.

(vi) Information gathering.
(vii) Payroll setup and verification.

3.2 Milestones to be Completed after Hand-Over Date – Human Resources Activities

The following activities will be completed after the Hand-Over Date consistent with the timeframes established in Schedule 2 *(Transition Plan)* to the Agreement:

(i) Knowledge Transfer
(ii) Staff Augmentation
(iii) Orientation and Acclimation

3.2.1 Knowledge Transfer

The purpose of activities relating to knowledge transfer is to facilitate the transfer of knowledge to the Service Provider Personnel from Province staff who are not transitioning to the Service Provider.

The Service Provider will:

(i) Document, with the cooperation of the Province, a process for the transfer of knowledge from Province staff, who are not transitioning to Service Provider's employment, to Service Provider Personnel.
(ii) Facilitate, with the cooperation of the Province, the transfer of knowledge to Service Provider Personnel from the said Province staff.

The Province will:

(i) Cooperate with the Service Provider as Service Provider documents the process and thereafter approve the documented process for the transfer of knowledge from Province staff, who are not transitioning to Service Provider's employment, to Service Provider Personnel.
(ii) Facilitate, with the cooperation of the Service Provider, the transfer of knowledge to Service Provider Personnel from the said Province staff.

3.2.2Augmentation of Province Staff

The purpose of staff augmentation activity is to coordinate efforts between the Province and the Service Provider to fill positions at the Province that will become vacant upon the Hand-Over Date.

The Service Provider will:

(i) Develop, in cooperation with the Province, a detailed staff augmentation plan for the Province vacant positions.
(ii) Participate prior to the Hand-Over Date, in the Province staffing process for vacant positions.
(iii) Undertake recruitment activities for staffing Province vacant positions.

The Province will:

(i) Prior to the Hand-Over Date, allow the Service Provider to participate in Province staffing activities for filling Province vacant positions.
(ii) Review and approve Service Provider proposed recruiting advertisements and communications related to Province vacant positions.
(iii) Provide all necessary written approvals and agreements with respect to those Province employees who are seconded to Service Provider.

3.2.3Orientation and Acclimation

The purpose of orientation and acclimation activities is to orient and acclimate employees new to the Service Provider, including transferred employees.

The Service Provider will:

(i) Establish plans for orientation and acclimation training including training with respect to Privacy Obligations.
(ii) Implement such plans prior to and following the Hand-Over Date.

The Province will:

(i) Cooperate with the Service Provider to enable agreed to orientation and acclimation training to take place prior to the Hand-Over Date.

4. Security Activities

4.1 Completed Milestones – Security Activities

Prior to the Hand-Over Date, the Province and the Service Provider have jointly prepared a policy gap analysis to determine differences between Province and Service Provider security policies.

5. Service Management Activities

5.1 Completed Milestones – Service Management Activities

The following activities have been completed by the Hand-Over Date:

(i) Province has provided preliminary Asset inventory lists as described in Schedule 22 (*Records Protocols*).
(ii) Province has provided authorization matrices and points of contact for the retained organization.
(iii) Province has supervised review of the existing Province operational manuals by the Service Provider.

6. Business Operations

6.1 Completed Milestones – Business Operations

The Province has identified Work-in-Progress Projects in effect prior to the Hand-Over Date or in contemplation. The Work-in-Progress Projects identified by the Province are listed in Schedule 4 *(Work-in-Progress Projects)* of the Agreement.

6.2 Milestones to be completed after Hand-Over Date – Business Operations

The following activities will be completed after the Hand-Over Date consistent with the timeframes established in Schedule 2 *(Transition Plan)* to the Agreement.

The Province and the Service Provider will evaluate the impact of Work-in-Progress Projects on the Transformation Plan during the initial refinement of the Transformation Plan described in Schedule 9 *(Transformation)*, Section 3.4. Changes to the Work-in-Progress Project Plans as a result of this evaluation will be developed in accordance with the Change Order Process.

7. Facilities Activities

7.1 Completed Milestones – Facilities Activities

The following activities have been completed by the Hand-Over Date:

(i) Lease by Service Provider of Service Provider Office facilities.

(ii) The arrangements between the Service Provider and the Province for Transitioning Employees (as defined in the Transformation SOW) for a three month period following the Hand-Over Date have been agreed and documented in Section 4 *(Office Facilities Transformation Project)* of the Transformation SOW

7.2 Milestones to be completed after Hand-Over Date – Facilities Activities

The following activity will be completed after the Hand-Over Date consistent with the timeframes established in Schedule 2 *(Transition Plan)* to the Agreement:

Service Provider's Subcontractor will enter into an agreement for the purchase of land or a building for STMS Interior Data Centre in accordance with the Agreement.

8.Subcontractor and Supplier Agreements

During the Transition, the Service Provider will finalize arrangements with its Material Subcontractors, other Suppliers and Subcontractors, as the case may be.

8.1 Material Subcontractors

The Service Provider will enter into Material Subcontractors with the following entitles on or prior to the Hand-Over Date and will provide such certificates to the Province to confirm that the Service Provider has entered into such subcontracts:

- Q9 Networks Inc.
- Myra Systems Corp.

8.2 Subcontractors and Suppliers

The Service Provider will enter into agreements with Subcontractors or Suppliers on or prior to the Hand-Over Date as required for the Service Provider to perform On Site Services at the Existing WTS Data Centres and Remote Sites after the Hand-Over Date.

9. Records Transferred from the Province to Service Provider

The Province will arrange with the Service Provider for the delivery of the Transferred Records to the Service Provider in accordance with the records protocols described in Schedule 22 *(Records Protocols)* to the Agreement.

Appendix A — Definitions

Capitalized terms used in this Schedule 3 that are not defined within this Schedule (including Appendix A) will have the meanings given to such terms in the Agreement or in Schedule 1 of the Agreement.

Definable Term	Definition
"BCGEU"	British Columbia Government Employee Union
"CRC"	Criminal Record Checks

SCHEDULE 4

WORK-IN-PROGRESS PROJECTS

The following table lists the Work-in-Progress Projects and their status as to the Hand-Over Date.

NAME OF WORK-IN-PROGRESS PROJECT	STATUS AT HAND-OVER-DATE
Veritas Bare Metal Restore	In Progress, approaching completion.
Distributed File System	In Progress, initiated over two years prior to the Hand-Over Date.
Migrate all servers running HP-UX to either Windows or Solaris servers during 2008.	In Progress, initiated over two years prior to the Hand-Over Date.
S. 15 At issue for Inquiry S. 15	In Progress, initiated over two years prior to the Hand-Over Date.
Citrix Farm S. 15 upgrade	In Progress.

SCHEDULE 5

SPECIAL TERMS

1. Section 4.2 (*Included or Inherent Services*) of the Agreement is supplemented as follows:

Notwithstanding the provisions of Section 4.2 (*Included or Inherent Services*) of the Agreement, if the Service Provider identifies a material function or a material task, after the Hand-Over Date, that:

(a) was performed prior to the Hand-Over Date by either the Province or a service provider for or on behalf of the Province; and

(b) was not disclosed (orally or in writing) by the Province to the Service Provider prior to the Hand-Over Date,

then the Service Provider will perform such material function or material task and the costs associated with the Service Provider's performance thereof shall be addressed through the Change Order Process. For the purposes of Section 4.2 (*Included or Inherent Services*) of the Agreement, a "material function" or "material task" shall mean a function or task for which, if the Service Provider were to charge the Province for the performance of the task of function using the Term of the Agreement using the Standard Time and Materials Rates set out in Schedule 23 (*Fees*), the Service Provider's charges to the Province would be greater than $100,000.

2. Section 4.4 (*Standard of Care*) of the Agreement is supplemented as follows:

For the first 12 months after the Hand-Over Date, the Service Provider shall be deemed to be providing the Services that are performed by the Transitioning Employees with the degree of care referred to in Section 4.4 (*Standard of Care*) of the Agreement, provided that:

(a) such Services that are performed by the Transitioning Employees are performed to at least the same degree of care as they were performed by such Transitioning Employees immediately prior to the Hand-Over Date; and

(b) the tasks and responsibilities performed by such Transitioning Employees after the Hand-Over Date are the same or substantially similar to the tasks and responsibilities performed by such Transitioning Employees after the Hand-Over Date.

3. Section 4.9(c) (*Manual Requirements)* of the Agreement is supplemented as follows:

The current documentation with respect to the Systems, business processes, and processes in support of the operations and procedures used to deliver the Services will be sufficient to enable the Province to have its personnel who are reasonably skilled in the provision of services similar to the Services.

4. Section 4.10 (*Knowledge Transfer*) of the Agreement is supplemented as follows:

For greater clarification, the knowledge transfer and level of information and detail required by the Province under Section 4.10 (*Knowledge Transfer*) of the Agreement shall be satisfied as follows:

(a) the Service Provider will:

(i) on an ongoing basis, make available to the Province all relevant Service Provider training materials relating to the Services (including, as appropriate, using electronic delivery of training materials and online courses);

(ii) provide timely updates of the Service Provider's perspective on related industry trends for the Province and Clients;

(iii) conduct a joint monthly review of a comprehensive set of metrics related to the Services; and

(iv) hold three, one-day, in depth reviews of at least three topical project issues for up to thirty Province employees; and

(b) the Service Provider and the Province address, in the Annual Operating Plan, the customized knowledge transfer required by the Province to be delivered by the Service Provider to the Province during the next year, having regard for the Service Provider's resource capacity, provided that the Service Provider will deliver no less that 150 hours of customized knowledge transfer to the Province in each year (which time shall not include time spent by the Service Provider in developing the customized materials). For greater certainty, any portion of the 150 hours not utilized during the year will not be rolled over into the next year.

5. Section 4.12 (*Failure of Province to Perform Retained Responsibilities*) of the Agreement is supplemented as follows:

(a) the first sentence of Section 4.12 (*Failure of Province to Perform Retained Responsibilities*) is supplemented to provide that in the event the Province fails to perform its obligations under the Agreement (other than a failure to make payment in accordance with Section 28.3 (*Material Breach by Province*)) and the Service Provider's performance of the Services is contingent upon the Province's performance of its obligations then, in addition to the other provisions of the first paragraph, paragraphs 4.12(a) – (h) apply;

(b) with respect to Section 4.12(a), the Service Provider STMS Lead and the Province STMS AMO Lead, will meet on a weekly basis, in person or by phone, to review the Service Provider issue tracking logs and identify Province failures or infringements, as contemplated under Section 4.12, that have occurred during such week, providing details with respect to such failure or infringement and if the Service Provider identifies, in such weekly review, Province failures or infringements then the weekly review shall constitute notice to the Province under Section 4.12(a);

(c) notwithstanding the provisions of Section 4.12(d) effective as of the actual date of the Province failure or infringement, the Service Provider and the Province will adjust the Fees, time frames for performance, Service Levels or Services, as applicable and to the extent affected, either on a temporary basis or a long term basis, in accordance with the Change Order Process; and

(d) in the event the Service Provider provides notice to the Province in accordance with Section 4.12(a) or as supplemented by Section 5(b) above, then the Service Provider and the Province will adjust the Fees, time frames for performance, Service Levels or Services, as applicable and to the extent affected, either on a temporary basis or a long

term basis, in accordance with the Change Order Process, effective as of the actual date of the Province failure or infringement (for greater certainty, and notwithstanding Section 4.12(e) of the Agreement, if the Service Provider fails to provide timely notice to the Province then any adjustment to the Fees, time frames for performance, Service Levels or Services, as applicable and to the extent affected, either on a temporary basis or a long term basis will be effective as of the date of notice actually provided by the Service Provider to the Province.

6. Section 7.5 (*Change Request Process*) of the Agreement is supplemented as follows:

In the event that a Province Change Request is complex (as determined below) and the Service Provider is *bona fide* not able to prepare a Proposal within ten (10) Business Days following receipt of a Province Change Request, then the Service Provider will prepare a preliminary Proposal ("**Preliminary Proposal**") within such ten (10) Business Day period, which Preliminary Proposal shall include a description of the following (to the extent applicable having regard to the nature of the proposed change):

(a) the time required to prepare a complete Proposal;

(b) the Fees payable by the Province to the Service Provider for the preparation of a complete Proposal;

(c) a high level assessment by the Service Provider of the impact on Services and the Service Levels, operations and Systems of the Service Provider used in the Services, Privacy Obligations and Fees payable by the Province should the Province elect to implement the change.

The Province will provide the Service Provider with a written response to the Preliminary Proposal within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process) of receipt of the Preliminary Proposal from the Service Provider, indicating:

(i) the Province's Approval of the Preliminary Proposal, in which case the Service Provider will prepare the related Proposal, within the time period set forth in the Preliminary Proposal (or such longer or shorter period of time as agreed to by the Parties), for the Province's further review in accordance with the provisions of Section 7.5 (*Change Request Process*) of the Agreement; or

(ii) the Province's rejection of the Preliminary Proposal (indicating the reasons therefor), in which case the Service Provider will not be required to provide any further information or services in connection with the Province's Change Request and the Province's Change Request will be deemed to be null and void; or

(iii) terms of a counter proposal acceptable to the Province, in which case, the provisions of Section 7.5 (*Change Request Process*) of the Agreement and, if applicable, this Section 6 of Schedule 5 (*Special Terms*) of the Agreement shall apply.

For the purposes of this Section 6, the determination whether a Province Change Request is complex will be made by the Province STMS AMO Lead and the Service Provider STMS Lead following the process set forth below:

(A) the Service Provider STMS Lead will promptly notify the STMS AMO Lead, that the Province Change Request is potentially "complex" having consideration for the work effort in terms of resources, cost or time for the Service Provider to prepare Proposal (for clarity, the Service Provider STMS Lead will provide details of the work effort in terms of resources, cost or time to the STMS AMO Lead);

(B) the STMS AMO Lead will confirm the intended scope of the Province's Change Request and the requirements thereof;

(C) the STMS AMO Lead and the Service Provider STMS Lead will discuss the intended scope of the Province's Change Request and requirements, as confirmed by the STMS AMO Lead; and

(D) the STMS AMO Lead will:

(1) approve the qualification of the Province Change Request as "complex", in which case the Service Provider will proceed with the preparation of a Preliminary Proposal, and the 10 Business Day period will commence upon the STMS AMO Lead;

(2) reject the qualification of the Province Change Request as "complex", in which case the STMS AMO Lead will either: (a) require the Service Provider to prepare a Proposal, and the 10 Business Day period will commence upon the STMS AMO Lead's rejection of the Province Change Request as "complex" or (b) will abandon the Change Request.

7. Section 7.8 (*Implementation of Mandatory Changes*) of the Agreement is supplemented as follows:

Upon the delivery of a Mandatory Change Request by the Province to the Service Provider, in accordance with Section 7.7 (*Mandatory Changes*) of the Agreement, the Parties shall comply with the following (as applicable to such Party):

(a) the Province shall promptly provide a written notice of meeting, with a copy of the Mandatory Change Request attached, to the members of the Joint Executive Committee, convening a meeting of the Joint Executive Committee within two (2) Business Days of the delivery by the Province of the Mandatory Change Request (or such later date that the members of the Joint Executive Committee so determine);

(b) the members of the Joint Executive Committee shall discuss and clarify the scope of such Mandatory Change Request, including any impact on the Fees, Service Levels, time frames, Privacy Obligations or the Services, to the extent known by the Parties at such time;

(c) with respect to the implementation of the Mandatory Change Request, the Service Provider shall not acquire any hardware, software or other assets for which the Province must reimburse the Service Provider, without the Province's prior written Approval; and

(d) the Service Provider shall provide copies of all invoices for services pertaining to any Mandatory Change to the Joint Executive Committee, promptly upon the issuance of such invoices, for review and approval of the Joint Executive Committee.

8. Section 7.8(e) (*Implementation of Mandatory Changes*) of the Agreement is supplemented as follows:

In the event of a Dispute between the Parties regarding the Province's adjustment to the Fees for a Mandatory Change, the Province will pay to the Service Provider that portion of the Fees for the Mandatory Change that are not the subject of the Dispute and any and all amounts in Dispute (the "**Disputed Fees**") will be borne by the Service Provider until such Dispute has been settled in accordance with paragraph 7.8(d)(iii) of the Agreement, provided that:

(a) amounts comprising the Disputed Fees will not exceed the amounts alleged to be in error or not properly invoiced or payable, or for which no Services were performed;

(b) the total amount of the Disputed Fees borne by the Service Provider shall not exceed, in the aggregate, one million dollars ($1,000,000);

(c) in the event that the total amount of the Disputed Fees is equal to one million dollars ($1,000,000), then any and all additional work performed by the Service Provider in connection with such Mandatory Change shall be charged by the Service Provider at the Standard Time and Materials Rates as set forth in Schedule 23 (*Fees*); and

(d) if the Province has a Dispute with respect to any and all additional work performed by the Service Provider in connection with such Mandatory Change in accordance with paragraph (c) above, then such Dispute will also be settled pursuant to the Dispute Resolution Process set forth in Article 26 (*Dispute Resolution)* provided that should the Dispute be referred to arbitration, the provisions of Section 27.3 (*Expedited Arbitration*) will apply.

In event of any settlement of a Dispute under Section 7.8 (*Implementation of Mandatory Changes*), as supplemented by this Section, which settlement is in favour of the Province, the Province may set-off the amount of such settlement, if any, against Fees and other charges payable by the Province to the Service Provider under this Agreement, or may deduct such amounts from any sum due or which at any time may become due to the Service Provider under this Agreement.

9. Section 7.8 (*Implementation of Mandatory Changes*) of the Agreement is supplemented as follows:

The Province shall not utilize a Mandatory Change Request or otherwise require the Service Provider to implement a Mandatory Change or Province directive for the purpose of resolving an existing Dispute for which any Dispute resolution process has been invoked between the Province and the Service Provider.

10. Section 9.1 (*Benchmarking*) of the Agreement is supplemented as follows:

The Benchmarker will not include: (a) the Transformed Services in the scope of the Benchmarking; and (b) the Transformation Fees or the Unit Price Adjustment (defined in Schedule 23 (*Fees*) in any benchmarking of the Fees.

11. Section 12.5 (*Non-Disclosure Documents*) of the Agreement is supplemented as follows:

The Province approves the External Personnel of Access Subcontractors entering into External Personal Agreements with the Access Subcontractor employing such External Personnel or to whom such External Personnel provide services and the Province shall not require that the External Personnel enter into External Personnel Agreements directly with the Service Provider.

12. Section 12.13 (*Removal of Subcontractor*) of the Agreement is supplemented as follows:

(a) for greater certainty, reference in Section 12.13(a) to "the Province having severed all other relationships with such Material Subcontractor" means the Province having severed a contract or subcontract with such Material Subcontractor; and

(b) Section 12.13(b) (*Removal of Subcontractor*) shall apply where there is an increased bona fide risk of a breach of the provisions of the *Freedom of Information and Protection of Privacy Act*, then:

(i) the Province shall notify the Service Provider, in writing, of such increased risk ("**Privacy Risk**"), identifying the particulars of such increased risk as known by the Province;

(ii) the Service Provider will cause the Access Subcontractor to cure the Privacy Risk within seven (7) days of receipt of notice from the Province, or such longer prior as the Parties may agree in writing; and

(iii) if the Access Subcontractor does not cure the Privacy Risk then the Province may require the Service Provider to replace the Access Subcontractor in accordance with the provisions of Section 12.13 (*Removal of Subcontractor*) of the Agreement.

13. Section 12.15(d) (*Suppliers*) of the Agreement is supplemented as follows:

Notwithstanding the provisions of Section 12.15(d) (*Suppliers*) of the Agreement, the Service Provider will not be liable for a failure of COTS software provided the Services Provider takes all reasonable steps and implements all reasonable measures to mitigate any Claims associated with such failed COTS software.

14. Section 15.4 (*Taxes*) of the Agreement is supplemented as follows:

Notwithstanding the provisions of Section 15.4 (*Taxes*) of the Agreement, the Province will be responsible for new Taxes that are imposed during the Term provided that such new Taxes are in the nature of sales, use, value added, goods and services, provincial sales or similar taxes imposed on Service Provider's products and services. For greater certainty, Service Provider is responsible for any and all Taxes, including new Taxes, impacting Service Provider's internal costs.

15. Section 16.3 (*Corporate Structure and Corporate Chart*) and Section 16.4 (*Canadian Entities*) of the Agreement is supplemented as follows:

With respect to Section 16.3 (*Corporate Structure and Corporate Chart*), the Province acknowledges that EDS Canada, the Performance Guarantor, is not Corporately Controlled by a Canadian Entity.

With respect to Section 16.4(b), the Province acknowledges that EDS Canada, Sun Microsystems of Canada Inc. and EMC Corporation of Canada are not Corporately Controlled by a Canadian Entity and the Province hereby Approves EDS Canada, Sun Microsystems of Canada Inc. and EMC Corporation of Canada as an Access Subcontractors.

The Service Provider will cause all Access Subcontractors to provide the Service Provider with immediate notice if, at any time during the Term, the Access Subcontractor is not in compliance with the provisions of Section 16.4 (*Canadian Entities*) or, subject to confidentially requirements, may not in the future be in compliance with provisions of Section 16.4 (*Canadian Entities*). Upon receipt of such notice from an Access Subcontractor, the Service Provider will:

(a) immediately notify the Province, in writing;

(b) obtain confirmation from the Access Subcontractor that the Access Subcontractor continues to be in compliance with the Privacy Obligations (other than provisions that are substantively the same as Section 16.4 (*Canadian Entities*)) and that such compliance will continue; and

(c) proceed with the orderly termination of the Access Subcontractor having regard for the Service Provider's ongoing service obligations to the Province and the potential risk of any breach of the provisions of Article 16 (*Privacy, Security and Confidentiality)*, other than Section 16.4 (*Canadian Entities*) and Schedule 24 (*Privacy Obligations*).

Provided that the Access Subcontractor is not in breach of the provisions of Article 16 (*Privacy, Security and Confidentiality*), other than Section 16.4 (*Canadian Entities*) or Schedule 24 (*Privacy Obligations*), then the Province will not have the right to terminate the Agreement, or any Services under the Agreement, on the basis that the Access Subcontractor is not in compliance with the provisions of Section 16.4 (*Canadian Entities*).

16. Section 16.6 (*Safeguarding Confidential Information*) of the Agreement is supplemented as follows:

For greater certainty, the Province agrees to protect the Service Provider Confidential Information that the Province receives with a degree of care that is no less that the degree of care used by the Province to protect its own confidential information.

17. Section 16.7(b) (*Permitted Disclosure and Use of Confidential Information*) of the Agreement is supplemented as follows:

For greater certainty, "professional advisors" of the Province includes the internal or external auditor, inspector, investigator, representative or other professional advisor appointed by the Province under Article 22 (*Audit*).

18. Section 16.8 (*Province Permitted Disclosure*), Article 22 (*Audit Rights*) and Section 29.2 (*Termination Assistance Plan*) of the Agreement are supplemented as follows:

The Province will not:

(a) disclose Service Provider Confidential Information under Section 16.8 (*Province Permitted Disclosure*) to a Competitor (defined below);

(b) utilize or engage a Competitor as the Province's auditor, investigator, inspector or authorized representatives, under Article 22 (*Audit Rights*); and

(c) utilize or engage a Competitor to assist with the development of a termination assistance plan for the transition of the Services from the Service Provider to the Province or an Alternative Service Provider, as contemplated under Section 29.2 (*Termination Assistance Plan*), provided that, the Province shall not be restricted from selecting any Competitor as its Alternative Service Provider, or otherwise release the Service Provider from its obligations under the Agreement or to cooperate with the Alternative Service Provider in the development of such termination assistance plan.

For the purposes of this Section 18 of Schedule (*Special Terms*), "Competitors" means

Notwithstanding the provisions of Article 16 (*Privacy, Security and Confidentiality*), the Province shall have the right to use and disclose the Service Provider Confidential Information received by the Province in connection with the Services or the Agreement to the Broader Public Sector entities that have entered into a BPS Services Agreement with the Service Provider. The Service Provider acknowledges and agrees that Service Provider Confidential Information may be shared among the Province and such Broader Public Sector entities, and may be used by the Province and such Broader Public Sector entities: (i) under their own Services Agreements as if such information had been disclosed to such party directly by the Service Provider; or (ii) in connection with the review, administration or operation of STMS, including in connection with any discussions with or among the Province and such Broader Public Sector entities of the Administrator relating to STMS.

19. Section 16.9(h) (*Exceptions to Obligation of Confidentiality*) of the Agreement is supplemented as follows:

The following information of the Service Provider and its Subcontractors constitutes highly confidential information: proprietary information; financial, technical or security information related to audits conducted under this Agreement or provided to the Financial Monitor; specific limits on liability as set forth in Schedule 31 (*Limits on Liability*) and Schedule 37 (*Remedies for Material Breach*) of the Agreement; information obtained on a tax return or gathered for the purpose of determining tax liability; and the Corporate Chart, except to the extent that such information is Province Confidential Information (collectively, the "**Highly Confidential Information**"). The Service Provider expressly advises the Province that the Highly Confidential Information contains trade secret, commercial and technical information of a highly sensitive nature, and such Highly Confidential Information has been supplied to the Province in confidence and the disclosure of the Highly Confidential Information would harm significantly the competitive position of the Service Provider, provide an unfair competitive advantage to its competitors and cause financial loss to the Service Provider. The provisions of Section 16.9(h) (*Exceptions to Obligation of Confidentiality*) shall not apply to Service Provider Highly Confidential Information.

20. Section 17.6 (*Testing of Business Continuity Plan)* of the Agreement is supplemented as follows:

(a) pursuant to Section 17.6(a) of the Agreement, the Service Provider will complete a test of the Business Continuity Plan not less than:

(i) 180 days after the Hand-Over Date, which test of the Business Continuity Plan shall consists of a process walkthrough and awareness testing; and

(ii) for each of the STMS Calgary Data Centre and the STMS Interior Data Centre, ninety (90) days after the Data Centre Availability Date for such STMS Data Centres;

(b) pursuant to Section 17.6(b) of the Agreement, the Service Provider will test the Business Continuity Plan annually following the initial test described in paragraph (a) above, within thirty (30) days of the anniversary date of the initial test; and

(c) pursuant to Section 17.6(f) of the Agreement, the Service Provider will complete a test of the Business Continuity Plan within thirty (30) days after implementing any material change in respect of the Services (including, without limitation, any material change in the technology, processes, facilities, infrastructure, Systems or Recovery Time Objectives), for purposes of determining the impact of such material changes to the Services and the effectiveness of the Business Continuity Plan in respect thereof.

21. Section 18.2 (*Technology Improvements and Currency*) of the Agreement is supplemented as follows:

Technology improvements identified by the Service Provider as required pursuant to Section 18.2 (*Technology Improvements and Currency*) of the Agreement shall be included in the Annual Operating Plan, under the heading "Technology Improvements and Currency").

22. Section 18.3 (*Material Technology Change*) of the Agreement is supplemented as follows:

The Province's Approval of any request by the Service Provider to change a material supplier of technology used by the Service Provider in performing the Services, will not be unreasonably withheld.

23. Section 18.5 (*System Contaminants*) of the Agreement is supplemented as follows:

Provided that neither the Service Provider nor its Subcontractors or Suppliers, is responsible for any Contaminant being introduced into any Systems used to provide the Services, the Service Provider will not be responsible for ensuring that the Systems that are used to provide the Services but that are owned, managed or controlled by the Province or a third party, do not and will not contain any Contaminant.

24. Article 22 (*Audit Rights*) of the Agreement is supplemented as follows:

(a) In each Contract Year the Province shall have the right to conduct:

(i) one (1) annual audit, the scope of which shall include any or all of the matters referred to in Section 22.4 (*Audit Right*), at the Province's discretion ("**Annual Audit**"); and

(ii) three (3) spot audits, the scope of which shall include specific matters referred to in Section 22.4 (*Audit Right*), at the Province's discretion (the "**Spot Audits**").

For greater certainty, any investigations and inspections pursuant to Section 22.3 (*Inspection and Investigation Rights*) are not included in, or counted toward, the Annual Audit or the Spot Audits.

(b) The costs of any Spot Audits will be dealt with in accordance with the following provisions:

(i) except as set forth in paragraph (ii)(A) below, the Province will pay its costs and expenses of any Spot Audits and the costs and expenses of any auditor or other professional advisor retained by the Province to conduct or assist with a Spot Audit including, for greater certainty, the Service Provider's (or its Subcontractors') costs incurred in connection with such Spot Audit, including the cost of the time and effort of the Service Provider and its Personnel, Subcontractors and External Personnel, at the Standard Time and Materials Rates, to comply with the requests and requirements of an, auditor or other professional advisor in respect of the same; and

(ii) where a Spot Audit reveals a material Deficiency (as determined by the Province, acting reasonably) as a result of the acts or omissions of the Service Provider (or of those Persons for whom the Service Provider is responsible at law or pursuant to the terms of this Agreement), then the following provisions will apply:

(A) upon correction of the material Deficiency so identified, and if so requested by the Province, the Service Provider will undertake a new audit, at the Service Provider's expense, to confirm that such material Deficiency has been fully addressed and remedied; and

(B) the Service Provider will promptly provide the results of such audit to the Province upon the Service Provider's receipt of the same.

(c) With respect to any Leveraged Systems used by the Service Provider in connection with the performance of the Services, to the extent that the Province Confidential Information is contained on such Leveraged Systems and is commingled with the information of other customers of the Service Provider, then:

(i) the auditor or other professional advisor retained by the Province to conduct or assist the audit shall have the right, at the Province's discretion, to:

(A) supervise the extraction of the Province Confidential Information from the commingled information; or

(B) perform the extraction of the Province Confidential Information from the commingled information as escorted and supervised by the Service Provider; or

(C) have the Service Provider extract the Province Confidential Information from the commingled information and provide the same to the Province, along with an officer's certificate, of a senior officer of the Service Provider, certifying that the extracted information

represents all of the Province Confidential Information requested by the Province, its auditor or professional advisor.

If, however, the Service Provider anticipates that providing the Province with the ability to supervise the extraction of or to extract the Province Confidential Information from the commingled information will provide the Province with such access to the commingled information that, were it another customer of the Service Provider requesting such access, the Province would object to the confidentiality of the Province Confidential Information contained therein being made available to an auditor, then the Service Provider will provide the Province with a detailed explanation of such circumstances and of the Service Provider's concerns. The Parties agree that, in such circumstances, the Service Provider will extract the Province Confidential Information from the commingled information and provide the same to the Province, along with a certificate of the Service Provider's auditor ("**Auditor's Certificate**") duly certifying any extraction of Province Confidential Information, certifying that the extracted information represents all of the Province Confidential Information requested by the Province, its auditor or professional advisor;

(ii) for highly sensitive Leveraged Systems of the Subcontractor performing the STMS Data Centre Services, where the disclosure of information would have an adverse impact on the security of the operations of the Subcontractor and its other customers of the STMS Data Centres ("**Sensitive Leveraged Systems**"), for example, video surveillance recordings, raw data supporting trouble tickets, access logs for the STMS Data Centres, records of security incidents, biometric records and shipping and receiving records and similar Leveraged Systems, the Service Provider will provide the Province with a certificate of the Service Provider's or Subcontractor's auditor ("**Auditor's Certificate**") duly certifying any extraction of Province Confidential Information from such Sensitive Leveraged Systems and certifying that the extracted information represents all of the Province Confidential Information requested by the Province, its auditor or professional advisor;

(iii) for highly sensitive security policies, where the disclosure of such policies would have an adverse impact on the security of the operations of the Service Provider or Subcontractor performing the STMS Data Centre Services and their respective customers, then:

(A) with respect to the Subcontractor performing the STMS Data Centre Services, the Service Provider will provide the Province with an Auditor's Certificate duly certifying the operation of the STMS Data Centre and the Data Centre Services are provided in compliance with Province Policies; and

(B) with respect to the Service Provider, the Service Provider will provide the auditor or the professional advisor retained by the Province to have access to review such security policies, at a Service Location, but for clarity, the auditor or the professional advisor shall not have the right to have copies of such highly sensitive security policies.

The auditor providing the Auditor's Certificate under this Section 24 must be a duly qualified Chartered Accountant in Canada, in good standing, with the requisite skills to carry out the tasks contemplated in this Section 24. In addition, the auditor shall provide the Province with details of the processes and procedures followed by the auditor in discharging the tasks contemplated in this Section 24 in order to prepare the Auditor's Certificate.

25. Section 20.3(f) (*Restrictions on Access and Use*) of the Agreement is supplemented as follows:

To the extent that the Province directs the Service Provider to take specific steps under Section 20.3(f) (*Restrictions on Access and Use*) to ensure that any adverse impact on the Province Shared Infrastructure is minimized or eliminated, and the Service Provider complies with the direction of the Province, then the Service Provider will not be responsible for any adverse impact on the Province Shared Infrastructure that results from the Service Provider's compliance with such Province direction.

26. Section 23.1(f) (*General Duties and Obligations of Service Provider*) of the Agreement is supplemented as follows:

If either the Party becomes aware of any amendments to any Privacy Laws (including any new Privacy Laws), such Party will notify the other Party of such change. If either Party concludes that compliance with such amendment will require any change to the Services or this Agreement, then the Service Provider will analyze the impact of the change on the Services or this Agreement, including the incremental costs that the Service Provider may incur as a result of such change, and such changes will be addressed through the Change Order Process. To the extent such change impacts other Service Provider clients, any additional costs will be apportioned on an equitable basis to all such clients, including the Province.

For the purposes of this Section 26, "Privacy Laws" means all Applicable Laws relating to data privacy, personal information or data, trans-border data flow and data protection.

27. Section 24.2 (*Service Provider Representations, Warranties and Covenants*) of the Agreement is supplemented as follows:

The representations, warranties or covenants contained in Section 24.2(c) and 24.2(e) relating to the jurisdiction of incorporation of the Performance Guarantor and Corporate Guarantor, respectively, are made by the Service Provider as of the date of this Agreement. In the event the jurisdiction of incorporation of the Performance Guarantor or the Corporate Guarantor changes during the Term of this Agreement, the Service Provider will promptly notify the Province and provide the Province with details of such change in jurisdiction, including the location of the new jurisdiction and other information reasonably requested by the Province.

The representations, warranties or covenants contained in Section 24.2(s) exclude the action filed in 2004 under No. C4 0879 in the Victoria Supreme Court under the style of cause: *British Columbia Government Employees Union v. The Minister of Health Services and the Medical Services Commission* and the petition filed on February 2, 2005 in the Supreme Court of British Columbia in the matter of the Judicial Review Procedure Act, between the B.C. Government and the Service Employees' Union and the Minister of Provincial Revenue.

The representations, warranties or covenants contained in Section 24.2(z) are made by the Service Provider as of the date of this Agreement. The Service Provider will notify the Province in the event becomes the Service Provider becomes aware of any material fact or matter not disclosed to the Province by the Service Provider which, if known by the Province, might be reasonably expected to deter the Province from entering into this Agreement or completing the transactions contemplated in this

Agreement and in the other Transaction Documents, or that might materially adversely affect the ability of the Service Provider to perform its obligations under this Agreement.

28. Section 28.1(f) (*Service Provider Material Breach*) of the Agreement is supplemented as follows:

Notwithstanding the provisions of Section 28.1(f) (*Service Provider Material Breach*), the following events shall not constitute a Material Breach of the Agreement by the Service Provider:

(a) the disclosure or use of Personal Information contrary to the provisions of *Freedom of Information and Protection of Privacy Act* (British Columbia) by the Transitioning Employees, where such disclosure or use of Personal Information occurs within the first six months after the Hand-Over Date; or

(b) the disclosure or use of Personal Information contrary to the provisions of *Freedom of Information and Protection of Privacy Act* (British Columbia) that occurs as a result of a hacker,

provided that in the case of both (a) and (b) above the Service Provider is not otherwise in breach of the provisions of Article 16 (*Privacy, Security and Confidentiality*) or Schedule 24 (*Privacy Obligations*). For the purposes of this Schedule 5 (*Special Terms*), the term "hacker" means a Person or Persons who commit, or circumvent computer security, unauthorized remote computer break-ins via a communication network such as the Internet or such similar unauthorized activities who is not Personnel or External Personnel of the Service Provider or a Subcontractor.

29. Section 28.1 (*Service Provider Material Breach*) of the Agreement is supplemented as follows:

In the event of a Material Breach of the Agreement by the Service Provider relating to Services, other than the Data Centre Services (and for the purposes of this Section 29, the Data Centre Services includes, Schedule 24 (*Privacy Obligations*) and the Security SOW, as those documents relate to the STMS Data Centres), then the Province will take an assignment of the Subcontract between the Service Provider and its Subcontractor, Q9 Networks Inc. ("**Province Assignment Obligation**"). The Province Assignment Obligation is subject to:

(a) the Province's right to approve amendments to the Subcontract between the Service Provider and Q9 Networks Inc. (the "**Q9 Subcontract**"), excluding amendments or change orders under the Q9 Subcontract that:

(i) are in the ordinary course of Service Provider's business of providing services to the Province or customers under a BPS Services Agreement; or

(ii) are the result of a requirement under the Agreement that the Service Provider must flow down certain provisions to the Subcontractor to meet the Service Provider's obligations to the Province,

provided that any amendments set forth in paragraphs (i) or (ii) above are consistent across the term of the Q9 Subcontract; and

(b) no obligations being triggered as a result of any assignment, or after any assignment, of the Q9 Subcontract, and in particular no special obligations (for example assignment fees or payments) on the Province as a result of the assignment of the Q9 Subcontract to the Province.

The Service Provider will provide to the Province, on a quarterly basis, a summary of any amendments to the Q9 Subcontract, including any ordinary course amendments or change orders.

30. Section 30.7 (*Effect of Labour Disruption*) of the Agreement is supplemented as follows:

The failure of the Service Provider to provide any Services as a result of the Province's Labour Disruption will not give rise to a breach of this Agreement by the Service Provider provided that the Service Provider makes all reasonable efforts to restore and perform the disrupted Services as soon as possible and the Service Provider continues to use all reasonable efforts to perform the disrupted Services during the continuance of the Province's Labour Disruption and until such disrupted Services are fully restored.

31. Section 30.8 (*Other Remedies)* of the Agreement is supplemented as follows:

In the event the Service Provider is unable or unwilling to restore any disrupted Services then, prior to procuring or otherwise obtaining Services from an alternative service provider, the Province will provide the Service Provider with ten (10) days notice, in writing, of its intention to procure or otherwise obtain services or goods from alternative service providers or suppliers.

Notwithstanding the provisions of Section 30.8(b) (*Other Remedies*) of the Agreement, if the failure of the Service Provider to provide any Services is as a result of the Province's Labour Disruption, then the Province shall not be entitled to off-set or deduct any costs that are in excess of the Fees withheld pursuant to Section 30.8(a) (*Other Remedies*) against any other Fees payable by the Province to the Service Provider under this Agreement or otherwise.

32. Section 31.1 (*Assignment by Province)* of the Agreement is supplemented as follows:

In the event the Province assigns the Agreement, in whole or in part, or sublicenses any right or benefit set forth in this Agreement (the "**Assigned Obligations**") to any government, public sector or Crown entity, body or authority (an "**Assignee**"), the Province shall not be relieved of its obligations under the Agreement to the extent the Assignee fails to perform any of the Assigned Obligations.

33. Section 32.3 (*Conflict of Interest)* of the Agreement is supplemented as follows:

Notwithstanding the provisions of Section 32.3 (*Conflict of Interest)* of the Agreement, the following activities will not give rise to or constitute a conflict of interest or perceived conflict of interest by the Service Provider or its personnel:

(a) any activities or business of the Service Provider, that is unrelated to the Agreement, with private sector entities;

(b) the marketing of hardware, software or other products or services, other than the Services, by the Service Provider to the Province or the Broader Public Sector;

(c) the marketing of the Services in accordance with the provisions of the Agreement, and in particular, the provisions of Schedule 26 (*Growth and Marketing*) of the Agreement;

(d) responding to any RFQ, RFI, RFP or other procurement document relating to hardware, software, or other products or services that may be issued by the Province or the Broader Public Sector, subject to providing the Province with prior written notice of the Service Provider's intention to respond to such RFQ, RFI, RFP or other procurement document,

provided that the Services Provider does not use any Province Confidential Information in connection with the activities described in paragraphs (a) – (d) above.

34. Section 33.6 (*No Liens or Charges against Provincial Assets*) of the Agreement is supplemented as follows:

The Parties acknowledge and agree that:

(a) Section 33.6 (*No Liens or Charges against Provincial Assets*) will not apply to the assets of, or used by, the DC Subcontractor (defined below), or its successor, in the provision of the Services and, in particular, the Province shall not require that such assets be kept free of any and all Liens; and

(b) no Lien or any action taken by any Person in respect of such Lien on any of the assets of, or used by, the DC Subcontractor, or its successor, shall release the Service Provider from its obligations to perform the Services or any of its obligations under the Agreement including any of the Service Level Agreements.

The provisions of Section 33.6 (*No Liens or Charges against Provincial Assets*) shall apply to the Service Provider DC Assets (defined below). The Service Provider acknowledges, and will cause any Subcontractor to acknowledge in writing upon request of the Province, that:

(i) the Service Provider is the owner of the Service Provider DC Assets now or hereafter located at or in the STMS Data Centres (or either STMS Data Centre);

(ii) the Subcontractor is not the owner of the Service Provider DC Assets located at or in the STMS Data Centres (or either STMS Data Centre); and

(iii) the Service Provider shall have unrestricted access to, and the right to repair, replace, remove or add Service Provider DC Assets located at or in the STMS Data Centres (or either STMS Data Centre) at the Service Provider's sole discretion at any time during the Term of this Agreement or upon the expiry or earlier termination of this Agreement, for any reason.

Without limiting the application of the foregoing, the Service Provider hereby acknowledges and agrees, and will cause any Subcontractor to acknowledge and agree in writing, that: (i) no right, title or interest in any Service Provider DC Assets is, or will be deemed to be acquired, by any Subcontractor, and (ii) the Service Provider DC Assets shall at all times be and remain the property of the Service Provider and shall not, under any circumstances be, or be deemed, a fixture or leasehold improvement to the STMS Data Centres (or either STMS Data Centre) at all times notwithstanding any fixation of such Service Provider DC Assets in or at the STMS Data Centres (or either STMS Data Centre).

Service Provider hereby consents, and will cause any Subcontractor to consent, to the registration by the Service Provider of financing statements in any provincial personal property registry where the Service Provider DC Assets may be located.

"**DC Subcontractor**" means Q9 Networks Inc.

"**Service Provider DC Assets**" means any and all assets that are purchased or leased by the Service Provider and used in the provision of the Services from the STMS Data Centres.

35. The Province and the Insurance Corporation of British Columbia ("**ICBC**") have entered into an agreement, the Participation Agreement, that, governs the relationship among the Province, ICBC, and any other Broader Public Sector entities obtaining services from the Service Provider under a Services Agreement including, the exercise by the Province, ICBC and such other Broader Public Sector entities (collectively, "**Customers**") of certain rights under their respective Services Agreements (the Agreement for the Province and the BPS Services Agreement for the Broader Public Sector entities). The Province, ICBC and any other Broader Public Sector entities obtaining services from the Service Provider under a Services Agreement are together "Buyers".

In particular, with respect to the following provisions of this Agreement, the Parties acknowledge and agree that, except as expressly set forth below:

(a) the Buyers will act in unison in connection with any exercise of the rights under the provisions below such that the rights under such provisions will be exercised collectively through the Administrator and not individually by the Buyers;

(b) the exercise of any rights under the provisions below will be through the Administrator on behalf of the Buyers; and

(c) the Service Provider shall rely upon the exercise of the rights under the provisions below by, and any instructions received from, the Administrator for all purposes, as if the exercise of such rights was by, and the instruction were from, all of the Customers:

(i) Section 2.8 (*One Year Extension*);

(ii) Section 5.3 (*Relocation of the Service Provider Service Locations*);

(iii) Section 7.7 (*Mandatory Changes*) and Section 7.8 (*Implementation of Mandatory Changes*), as supplemented by Sections 7 and 8 of this Schedule 5, to the extent that such Mandatory Change affects the Province and one or more of the other Customers;

(iv) Section 8.5 (*Review and Changes to Service Levels*);

(v) Section 8.9 (*Service Level Failures*) and in particular, Section 8.9(b), the procurement of, or otherwise obtaining, services or goods from any alternative service providers or suppliers;

(vi) Article 9 (*Benchmarking*);

(vii) Section 11.4 (*Customer's Right to Issue Directives*), to the extent that the exercise of such right by the Province affects one or more of the Province and one or more of the other Customers;

(viii) Section 11.7 (*Changes in Key Positions*);

(ix) Section 11.8 (*Key Position Failures*);

(x) Section 12.9 (*Additional Material Subcontract Terms*);

(xi) Section 12.11 (*Consent to Use of Material Subcontractors*);

(xii) Article 22 (*Audit Rights*), as supplemented by Section 18 above, and in particular, the Customer acknowledges that the right to trigger an Annual Audit and any Spot Audits shall be exercised by the Administrator on behalf of the Customer;

(xiii) Article 27 (*Dispute Resolution*) where any Dispute affects the Customer and one of more of the Province and one or more of the other Customers;

(xiv) Section 30.4(b) (*Consequences of Force Majeure Event*) with respect to the procurement of, or otherwise obtaining, alternative Services from any Person during the period of time that the Force Majeure Event remains in effect;

(xv) Section 30.8(b) (*Other Remedies*) with respect to the procurement of, or otherwise obtaining, alternative Services from any Person in replacement for or substitution of the affected Services during the period of time that the Labour Disruption is in effect;

(xvi) Section 31.2 (*Assignment by Service Provider*) with respect to any consent given or withheld in connection with Sections 31.2(a) and (d); and

(xvii) the appointment of the Designated Representative under Schedule 24 (*Privacy Obligations*) of the Agreement.

36. Except in respect of any remedy in this Agreement which is expressly described as the exclusive remedy in respect of a matter, the rights and remedies of a Party in the Agreement are cumulative and in addition to and not in substitution for any right or remedy that may be available to a Party and the exercise of a right or remedy shall not exhaust all rights and remedies or prevent a Party from exercising any one or more of such rights or remedies or any combination of remedies and rights, thereafter or any of them simultaneously.

SCHEDULE 6

BASIC SERVICES

The Services to be provided by the Service Provider to the Province are more particularly described in the following Statements of Work (each also referred to as a "**SOW**"):

SOW	**Document Number**
SOW 1 – Transition Services dated March 30, 2009	Refer to Schedule 2 (*Transition Plan*)
SOW 2 – Data Centre Services dated March 30, 2009	50653542.4
SOW 3 – Security Services dated March 30, 2009	50653257.2
SOW 4 – Managed Mainframe Services dated March 30, 2009	50648830.7
SOW 5 – Midrange	
SOW 5A – Server Management Services dated March 30, 2009	50651178.5
SOW 5B – Shared File and Print Services dated March 30, 2009	50651509.3
SOW 5C – Web Hosting Services dated March 30, 2009	50651908.2
SOW 5D – Virtual Hosting Services dated March 30, 2009	50651713.3
SOW 5E – Onsite Support Services dated March 30, 2009	50651204.3
SOW 5F – Citrix Based Computing Services dated March 30, 2009	50651915.4
SOW 5G – Shared Database Services dated March 30, 2009	50651898.3
SOW 5H – Application Enabling Services dated March 30, 2009	50651913.2
SOW 6 – Storage and Backup Services dated March 30, 2009	50649290.7
SOW 7 – Service Management Services dated March 30, 2009	50660084.4
SOW 8 – Business Continuity and Disaster Recovery Services dated March 30, 2009	50652876.6

SOW 1 – TRANSITION SERVICES

See Schedule 2 (*Transition Plan*).

SOW 2 - Data Centre Services Statement of Work

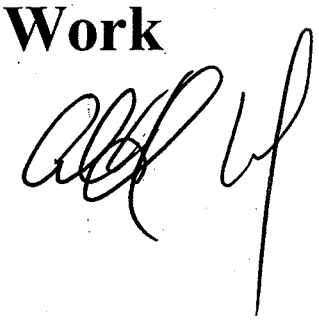


TABLE OF CONTENTS

DATA CENTRE SERVICE SOW # 2

Scope and Summary of Data Centre Services

I INTRODUCTION

The Data Centre Services Statement of Work (the "**Statement of Work**" or "**SOW**") is entered into pursuant to the Master Services Agreement between Her Majesty the Queen in right of the Province of British Columbia, as represented by the Minister of Labour and Citizens' Services (the "**Province**") and EDS Advanced Solutions Inc. ("**Service Provider**" or "**SP**"). Such Master Services Agreement, as amended, is referred to in this Statement of Work as the "**Agreement**".

The Data Centre Services Statement of Work consists of following additional parts:

(i) Part II – Existing WTS Data Centres Services;
(ii) Part III – WTS Remote Sites Services;
(iii) Part IV – Network Services;
(iv) Part V – STMS Data Centres Services; and
(v) Part VI – Media Destruction and Equipment Disposal Services.

This Statement of Work includes the following appendices:

- Appendix A – Defined Terms / Definitions
- Appendix B – Reports
- Appendix C – STMS Hosting Tools and Common Infrastructure Expected VA Consumption
- Appendix D – Supported Province Locations
- Appendix E – Service Provider Service Locations
- Appendix F – WTS Data Centre Infrastructure Capacity Request/Approval Process
- Appendix G – Data Centre Requirements
- Appendix H – Energy and Environmental Efficiency

1.1 Definitions

Certain capitalized terms used in this Statement of Work are defined in Appendix A (*Defined Terms/Definitions*) of this Statement of Work. Capitalized terms used in this Statement of Work that are not defined within this Statement of Work (including in Appendix A) will have the meanings given to such terms in Schedule 1 of the Agreement.

1.2 Purpose of this Document

This SOW describes the scope and functions of the Data Centre Services being performed by Service Provider in accordance with the terms of the Agreement and the Province's responsibilities in connection therewith.

1.3 Overview

This SOW describes, in detail:

(i) in Part II, the manner in which the Service Provider is authorized to use and the provisions applicable to the Service Provider's use of the data centre facilities (the "**Existing WTS Data Centres**") identified in Part II of Appendix D (*Supported Province Locations*) in providing Services under the Agreement;

(ii) in Part III, the manner in which the Service Provider is authorized to use and the provisions applicable to the Service Provider's use of the remote site facilities (the "**WTS Remote Sites**") identified in Part III of Appendix D (*Supported Province Locations*) in providing Services under the Agreement;

(iii) in Part IV, the network services to be provided by the Service Provider in connection with the Services Provider's use of data centre facilities and remote sites;

(iv) in Part V, the data centre services to be provided by the Service Provider from the data centre facilities (the "**STMS Data Centres**") identified in Part V of Appendix E (*Service Provider Service Locations*);

(v) in Part VI, the media destruction and equipment disposal services to be provided by the Service Provider at the Existing WTS Data Centres, WTS Remote Sites, and STMS Data Centres;

and the responsibilities of the Province in connection therewith.

1.4 Use of RASIC Table

The RASIC tables in this SOW set forth the responsibilities of the Service Provider and the Province for specific service elements within a service component. The RASIC tables are populated with responsibility indicators as follows:

- **R**esponsible: solely and directly accountable for creating a work product
- **A**pproving: needs to review and assure this work product's quality
- **S**upporting: any and all individuals or groups who help create this work product
- **I**nformed: any and all who need updates during the creation of a work product or during the execution of a business process
- **C**onsulted: any and all who help define product design or quality review criteria

These tables summarize key high-level responsibilities for various items related to the STMS Data Centres.

1.5 Common Functions

This Statement of Work contains references to services, activities, procedures or responsibilities that are defined in other Statements of Work including the *Service Management Services SOW*, the *Transformation SOW*, the *Business Continuity and Disaster Recovery Services SOW*, the *Security Services SOW*, the *Managed Mainframe Services SOW*, the eight (8) Midrange Services SOWs (*Server Management Services SOW*, *Shared File and Print Services SOW*, *Web Hosting Services SOW*, *Virtual Hosting Services SOW*, *Onsite Support Services SOW*, *Citrix Based Computing Services SOW*, *Shared Database Services SOW*, and the *Application Enabling*

Services SOW), and the *Storage and Backup Services SOW* entered into pursuant to the Agreement.

II EXISTING WTS DATA CENTRES SERVICES

This Part II of the Data Centre Services SOW identities the manner in which the Service Provider is authorized to use and the provisions applicable to the Service Provider's use of the Existing WTS Data Centres in providing Services under the Agreement.

This Part II of the Data Centre Services SOW is divided into two additional sections:

(i) Section 1 of this Part II of the Data Centre Services SOW provides an introduction to the services; and

(ii) Section 2 of this Part II of the Data Centre Services SOW describes the data centre services to be provided for the Existing WTS Data Centres (the "**Existing WTS Data Centres Services**").

1. Introduction

1.1 Sites

The Existing WTS Data Centres Services will be provided from the Existing WTS Data Centres.

1.2 Effective Date and Term

This Part II of the Data Centre Services SOW will be effective with respect to each Existing WTS Data Centre on the Hand-Over Date and will continue in effect:

(i) with respect to each Existing WTS Data Centre other than the Province Designated Network Locations, until such time (the "**WTS Data Centres Equipment End Date**") as all WTS Data Centres Equipment is removed from the Existing WTS Data Centre (1) in accordance with the Part VI (*Media Destruction and Equipment Disposal*) of the Data Centre Services SOW (for equipment that is being disposed of), (2) pursuant to the Virtualization and Migration Project described in Part 16 of the Transformation SOW (for equipment that is being relocated to the STMS Data Centres); or (3) pursuant to a Change Order entered into by the Parties under the Change Order Process; and

(ii) with respect to each of the Existing WTS Data Centres that is a Province Designated Network Location, until the later of: (1) the WTS Data Centres Equipment End Date for such data centre; and (2) the date that any routers or other communications equipment of the Service Provider installed at such data centre in accordance with Part IV (*Network Services*) of the Data Centre Services SOW are removed by the Service Provider.

1.3 Related SOWs or Schedules

1.3.1 Business Continuity/Disaster Recovery

The business continuity and disaster recovery services to be provided by the Service Provider for the services that the Service Provider is providing under this Part II of the Data Centre Services SOW are described in the *Business Continuity and Disaster Recovery Services SOW*.

2. *Existing WTS Data Centres Services*

This section describes the responsibilities of the Service Provider and the Province in respect of each Existing WTS Data Centre during the period that this Part II of the Data Centre Services SOW continues in effect with respect to such Existing WTS Data Centre in accordance with Section 1.2 (*Effective Date and Term*) of this Part II of the Data Centre Services SOW.

For each Existing WTS Data Centre:

(i) the Service Provider will utilize the site for the purpose of providing the Managed Services for the WTS Data Centres Equipment located at the site in accordance with the access, security, safety, operations and facility procedures of the Province and, subject to Part IV (*Network Services*) of the Data Centre Services SOW, for no other purpose; and

(ii) the Province will be responsible for the physical site, its ongoing facility operations, and the Province LAN services within the sites. The Province's responsibility for ongoing facility operations covers responsibility for items such as rent, utilities, maintenance and repairs to HVAC, UPS, generators, fire protection, security and the installation of server enclosures, power outlets, structured cabling, cable trays and copper patch cords.

Responsibility	Province	Service Provider
Provide to the Service Provider the work space at each of the Existing WTS Data Centres that is identified in Part II of Appendix D (if any). Such work space is provided on an "as available" basis. The work space shall include phone, network connectivity to SPAN/BC, internet connectivity and heat, light, ventilation, electric current and outlets for use by Service Provider. The work space shall be safe, clean and in compliance with Applicable Laws.	R	
Provide the Service Provider, on or prior to Hand-Over Date, with copies of all existing Province Policies regarding access, security, safety, operations and facility procedures in effect at the Existing WTS Data Centres.	R	
Notify the Service Provider of any updates to the Province Policies regarding access, security, safety, operations and facility procedures at the Existing WTS Data Centres occurring after the Hand-Over Date through the Change Order Process.	R	
Provide access control and security services in respect of each Existing WTS Data Centre in accordance with the Province Policies relating thereto that are in effect at such data centre.	R	

Responsibility	Province	Service Provider
Notify the Province in writing of Service Provider personnel requiring access to the Existing WTS Data Centres after the Hand-Over Date in order for the Service Provider to perform the Managed Services for the WTS Data Centres Equipment located at such data centres.		R
Notify the Province in writing of any Service Provider personnel no longer requiring access to the Existing WTS Data Centres within 5 Business Days of the date such access is no longer required.		R
Provide the Service Provider, immediately after the Hand-Over Date and for each Existing WTS Data Centre, building layouts and emergency safety documentation and a facility orientation.	R	
Provide the Service Provider with any updates to the building layouts of or emergency safety documentation for an Existing WTS Data Centre made after the Hand-Over Date promptly after such updates are implemented at the Existing WTS Data Centre.	R	
Provide the Service Provider with access to the Existing WTS Data Centres and to the WTS Data Centres Equipment and the Service Provider Network Equipment located at the data centre as required by the Service Provider to perform the Managed Services for such WTS Data Centres Equipment and Service Provider Network Equipment.	R	
Adhere to Province Policies regarding access, security, safety, operations and facility procedures at the Existing WTS Data Centres in effect at the Hand-Over Date or as updated thereafter and of which Service Provider is given notice in accordance with this Part II of the Data Centre Services SOW.		R
Notify the Service Provider in writing of Province onsite contact personnel for each Existing WTS Data Centre who can respond to facility related questions and incidents and of any changes to the list of Province onsite contact personnel.	R	
Monitor temperature, humidity, electrical power and related indicators of the facilities environment at each Existing WTS Data Centre.	R	
Resolve and manage facility environmental incidents within each Existing WTS Data Centre with a view to minimizing the impact on the availability, accessibility and operations of the Existing WTS Data Centres.	R	

Responsibility	Province	Service Provider
Notify Service Provider of facility environmental incidents or network incidents at each Existing WTS Data Centre that impact or could potentially impact the WTS Data Centres Equipment or Service Provider Network Equipment or the ability of the Service Provider to perform the Managed Services for such WTS Data Centres Equipment or the Service Provider Network Equipment.	R	
Provide corrective action updates and final resolution to Service Provider in the same timeframe as defined (by incident priority) in the Service Management SOW on all facility environmental incidents and all network incidents at each Existing WTS Data Centre that impact or could potentially impact the WTS Data Centres Equipment or the Service Provider Network Equipment or the ability of the Service Provider to perform the Managed Services for such WTS Data Centres Equipment or the Service Provider Network Equipment.	R	
Notify the Province in writing, with respect to each Existing WTS Data Centre, of the Service Provider Personnel to be contacted when a facility environmental incident or network incident occurs at the Existing WTS Data Centre and provide the Province with updates to such list of Service Provider Personnel promptly after the updates are effective.		R
Maintain the facility infrastructure within each Existing WTS Data Centre such that: (i) the equipment for environmental systems at the Existing WTS Data Centre (including the power systems, HVAC systems, fire detection and prevention systems and security systems) is maintained in accordance with the equipment manufacturer's specifications; and (ii) the facility is maintained in accordance with the requirements of applicable authorities having jurisdiction.	R	
Provide planning and management for any upgrades to the environmental systems at the Existing WTS Data Centres (including power systems, HVAC systems, fire detection and prevention systems and security systems).	R	

Responsibility	Province	Service Provider
Notify Service Provider of any facility maintenance or upgrade event that impacts or could potentially impact the WTS Data Centres Equipment or the Service Provider Network Equipment at an Existing WTS Data Centre or the ability of the Service Provider to perform the Managed Services for such WTS Data Centres Equipment or the Service Provider Network Equipment at the Existing WTS Data Centre in performing the Services.	R	
Provide the Service Provider with weekly power capacity reporting for the Existing WTS Data Centres as required by the Service Provider in managing the WTS Data Centres Equipment and the Service Provider Network Equipment. Such weekly power capacity reporting will be provided using the "Current Data Centre Load Charts" identified in Appendix B or such other reports as provide substantially the same information.	R	
Notify the Service Provider of the criteria that will be applied by the Province to approve or reject requests for changes in WTS Data Centres Equipment or the Service Provider Network Equipment at the Existing WTS Data Centres and any changes in the Province's current process for requesting such approvals. (The current WTS process for requesting approval of equipment changes is set out in Appendix F (*Data Centre Infrastructure Capacity Request/Approval Process*)).	R	
Request approval from the Province of planned WTS Data Centres Equipment or Service Provider Network Equipment changes (adds, moves, changes, and deletes) utilizing the Province's current process therefor.		R
Approve or reject Service Provider requests for planned equipment changes at each Existing WTS Data Centre within 2 Business Days of Service Provider's request for approval in accordance with the criteria identified by the Province.	R	
In connection with the Services being provided for the WTS Data Centres Equipment or the Service Provider Network Equipment, request adds, moves, changes, and deletes of power outlets, LAN ports, VLAN configuration changes, IP addressing, routing, Access Control Lists ("**ACL**"), structured cabling, cable trays, server enclosures, rack power bars, and seismic restraining to be provided by the Province at Existing WTS Data Centres.		R

Responsibility	Province	Service Provider
Approve or reject requests of the Service Provider for adds, moves, changes, and deletes of power outlets, LAN ports, VLAN configuration changes, IP addressing, routing, ACL, structured cabling, cable trays, server enclosures, rack power bars, and seismic restraining at Existing WTS Data Centres within three Business Days of the request and based on the criteria for such adds, moves, changes and deletes of which the Province has given Service Provider notice.	R	
Perform adds, moves, changes, and deletes of power outlets, structured cabling, cable trays, server enclosures, rack power bars, and seismic restraining at Existing WTS Data Centres in accordance with requests of the Service Provider that have been approved by the Province within 2 weeks of the request.	R	
Provide all requested LAN ports, VLAN configuration changes, IP addressing, routing, ACL in accordance with requests of the Service Provider that have been approved by the Province within 2 weeks of the request.	R	
Provide and install fibre patch cords.		R
Supply, manage and support all network hardware, network software, and network configurations within the Existing WTS Data Centres (other than as provided by the Service Provider in Part IV (*Network Services*) of the Data Centre Services SOW) as required by the applications operating on the WTS Data Centres Equipment and to enable the Service Provider to communicate with and support the WTS Data Centres Equipment as part of the Managed Services.	R	
Monitor network capacity of LAN, router, and firewall infrastructure components within the Existing WTS Data Centres and supply, install and support new network hardware such as routers, switches and firewalls when additional port, bandwidth or firewall capacity is required by the applications operating on the WTS Data Centres Equipment and to enable the Service Provider to communicate with and support the WTS Data Centres Equipment as part of the Managed Services.	R	
Monitor network performance within the Existing WTS Data Centres and upgrade network components such as routers, switches, firewalls, network cabling and carrier lines when additional performance and/or speed is required by the applications operating on the WTS Data Centres Equipment and to enable the Service Provider to communicate with and support the WTS Data Centres Equipment as part of the Managed Services.	R	

Responsibility	Province	Service Provider
Refresh the network hardware and software provided by the Province at the Existing WTS Data Centres when it reaches the end of its asset life or when the hardware / software is no longer supported by a maintenance agreement.	R	
Notify Service Provider of any network maintenance or upgrade event that impacts or could potentially impact the WTS Data Centres Equipment or the Network Equipment or the ability of the Service Provider to perform the Managed Services for such WTS Data Centres Equipment or the Network Equipment.	R	
Upon request by the Service Provider, provide such network capacity and network performance reports as are available within 5 Business Days of the Service Provider's request. (The reports will be used to help diagnose issues and/or problems with the Service supplied by the Service Provider.)	R	
Provide and install blank out panels into unused portions of server enclosures installed by the Service Provider at Existing WTS Data Centres.		R
Provide the quantity of copper patch cords at Existing WTS Data Centres required by Service Provider to perform Services.	R	
Install copper patch cords between WTS Data Centres Equipment and LAN ports provided by the Province.		R
Notify Province of any MAC address change relating to the WTS Data Centres Equipment that occurs within the Existing WTS Data Centres.		R
Where reasonably possible and with 3 Business Day's prior notice, accept delivery and securely store WTS Data Centres Equipment or the Service Provider Network Equipment at the Province's loading dock at S. 15 for up to one Business Day from the time the Province has accepted delivery.	R	
Remove WTS Data Centres Equipment or Service Provider Network Equipment temporarily received and stored at the Province's loading dock at S. 15 within one Business Day from the time that the Province has accepted delivery.		R
Transport WTS Data Centres Equipment or the Service Provider Network Equipment to Existing WTS Data Centres (other than S. 15) for installation.		R
Provide access to garbage and recycling facilities for disposal of packing material at each Existing WTS Data Centre.	R	

Responsibility	Province	Service Provider
For any WTS Data Centres Equipment or Service Provider Network Equipment brought to an Existing WTS Data Centre by the Service Provider, remove packing material from the Existing WTS Data Centre or dispose of packing material in garbage and recycling facilities at the Existing WTS Data Centre provided by the Province.		R
Review power, cooling air flow and cabling installation of WTS Data Centres Equipment or Service Provider Network Equipment performed by Service Provider at each Existing WTS Data Centre and notify Service Provider of any corrections in such installations required to remedy deficiencies.	R	
Remedy any WTS Data Centres Equipment or Service Provider Network Equipment installation deficiencies with regards to power, cooling air flow and cabling of which Service Provider is notified by the Province.		R
For each Existing WTS Data Centre, once all WTS Data Centres Equipment and any Service Provider Network Equipment located at the Existing WTS Data Centre has been removed, notify the Province network group, through an ITIMS order, to have the remaining Province supported network components (WAN and LAN) decommissioned as appropriate at the site.		R
Remove Service Provider access privileges to each Existing WTS Data Centre as requested within 5 Business Days of the request.	R	

III WTS REMOTE SITES SERVICES

This Part III of the Data Centre Services SOW identities the manner in which the Service Provider is authorized to use and the provisions applicable to the Service Provider's use of the WTS Remote Sites in providing Services under the Agreement.

This Part III of the Data Centre Services SOW is divided into two additional sections:

(i) Section 1 of this Part III of the Data Centre Services SOW provides an introduction to the services; and

(ii) Section 2 of this Part III of the Data Centre Services SOW describes the remote services to be provided for the WTS Remote Sites (the "**WTS Remote Sites Services**").

1. Introduction

1.1 Sites

The WTS Remote Sites Services will be provided from the WTS Remote Sites.

1.2 Effective Date and Term

This Part III of the Data Centre Services SOW will be effective with respect to each WTS Remote Site on the Hand-Over Date. This Part III of the Data Centre Services SOW will continue in effect:

(i) with respect to each WTS Remote Site until such time (the "**WTS Remote Sites Equipment End Date**") as all WTS Remote Sites Equipment is removed from the WTS Remote Site: (1) in accordance with Part VI (*Media Destruction and Equipment Disposal*) of the Data Centre Services SOW (for equipment that is being disposed of); (2) pursuant to the Transformation SOW (for equipment that is being relocated to the STMS Data Centres); or (3) pursuant to a Change Order entered into by the Parties under the Change Order Process.

1.3 Related SOWs or Schedules

1.3.1 Business Continuity/Disaster Recovery

The business continuity and disaster recovery services to be provided by the Service Provider for the services that the Service Provider is providing under this Part III of the Data Centre Services SOW are described in the *Business Continuity and Disaster Recovery Service SOW*.

2. WTS Remote Sites Services

This section describes the responsibilities of the Service Provider and the Province in respect of each WTS Remote Site during the period that this Part III of the Data Centre Services SOW continues in effect with respect to such WTS Remote Site in accordance with Section 1.2 (*Effective Date and Term*) of this Part III of the Data Centre Services SOW.

For each WTS Remote Site:

(i) the Service Provider will utilize the site for the purpose of providing the Managed Services for the WTS Remote Sites Equipment located at the site in accordance with the access, security, safety, operations and facility procedures of the Province and, subject to Part IV (*Network Services*) of the Data Centre Services SOW, for no other purpose; and

(ii) the Province will be responsible for the physical site (at both existing and new sites) and its ongoing facility operations. The ongoing facility operations covers items such as rent, utilities, maintenance and repairs to HVAC, UPS, generators, fire protection, security and the installation of server enclosures, power outlets, structured cabling, and cable trays.

Responsibility	Province	Service Provider
Provide to the Service Provider work space at each of the WTS Remote Sites, to the extent such work space exists as at the Hand-Over Date, as required by the Service Provider to perform the Managed Services for the WTS Remote Sites Equipment located at such site. The work space shall be safe, clean and in compliance with Applicable Laws.	R	
Provide the Service Provider, on or prior to Hand-Over Date, with copies of all existing Province Policies regarding access, security, safety, operations and facility procedures in effect at the WTS Remote Sites.	R	
Notify the Service Provider of any updates to the Province Policies regarding access, security, safety, operations and facility procedures at the WTS Remote Sites occurring after the Hand-Over Date through the Change Order Process.	R	
Provide access control and security services in respect of each WTS Remote Site in accordance with the Province Policies relating thereto that are in effect at such site.	R	
Notify the Province in writing of Service Provider personnel requiring access to the WTS Remote Sites after the Hand-Over Date in order for the Service Provider to perform the Managed Services for the WTS Remote Sites Equipment located at such site.		R
Notify the Province in writing of any Service Provider personnel no longer requiring access to a WTS Remote Site within 5 Business Days of the date such access is no longer required.		R
Provide the Service Provider, immediately after the Hand-Over Date and for each WTS Remote Site, building layouts and emergency safety documentation and a facility orientation.	R	
Provide the Service Provider with any updates to building layouts of or emergency safety documentation for a WTS Remote Site made after the Hand-Over Date promptly after such updates are implemented at the WTS Remote Site.	R	
Provide the Service Provider with access to the WTS Remote Site and to the WTS Remote Sites Equipment located at the site as required by the Service Provider to perform the Managed Services for such WTS Remote Sites Equipment.	R	

Responsibility	Province	Service Provider
Adhere to Province Policies regarding access, security, safety, operations and facility procedures at the WTS Remote Sites in effect at the Hand-Over Date or as updated thereafter and of which Service Provider is given notice in accordance with this Part III of the Data Centre Services SOW.		R
Notify the Service Provider of Province contact personnel for each WTS Remote Site who can respond to facility related questions and incidents and of any changes to the list of Province contact personnel.	R	
Monitor temperature, humidity, electrical power and related indicators of the facilities environment at each WTS Remote Site.	R	
Resolve and manage facility environmental incidents within each WTS Remote Site with a view to minimizing the impact on the availability, accessibility and operations of the WTS Remote Sites.	R	
Notify Service Provider of facility environmental incidents or network incidents at each WTS Remote Site that impact or could potentially impact the WTS Remote Sites Equipment or the ability of the Service Provider to perform the Managed Services for such WTS Remote Sites Equipment.	R	
Provide corrective action updates and final resolution to Service Provider in the same timeframe as defined (by incident priority) in the Service Management SOW on all facility environmental incidents and all network incidents at each WTS Remote Site that impact or could potentially impact the WTS Remote Sites Equipment or the ability of the Service Provider to perform the Managed Services for such WTS Remote Sites Equipment.	R	
Notify the Province in writing, with respect to each WTS Remote Site, of the Service Provider Personnel to be contacted when a facility environmental incident or network incident occurs at the WTS Remote Site and provide the Province with updates to such list of Service Provider Personnel promptly after the updates are effective.		R

Responsibility	Province	Service Provider
Maintain the facility infrastructure within each WTS Remote Site such that: (i) the equipment for environmental systems at the WTS Remote Sites (including the power systems, HVAC systems, fire detection and prevention systems and security systems) is maintained in accordance with the equipment manufacturer's specifications; and (ii) the facility is maintained in accordance with the requirements of applicable authorities having jurisdiction.	R	
Provide planning and management for any upgrades to the environmental systems at the WTS Remote Sites (including power systems, HVAC systems, fire detection and prevention systems and security systems).	R	
Notify Service Provider of any facility maintenance or upgrade event that impacts or could potentially impact the WTS Remote Sites Equipment at a WTS Remote Site or the ability of the Service Provider to perform the Managed Services for such WTS Remote Sites Equipment.	R	
Provide the Service Provider with weekly power capacity reporting for the WTS Remote Sites identified as a Regional Network Centre in Part III of Appendix D (*Supported Province Locations*) as required by the Service Provider in managing the WTS Remote Sites Equipment. Such weekly power capacity reporting will be provided using the "Current Data Centre Load Charts" identified in Appendix B or such other reports as provide substantially the same information.	R	
Notify the Service Provider of the criteria that will be applied by the Province to approve or reject requests for changes in WTS Remote Sites Equipment at the WTS Remote Sites and any changes in the Province's current process for requesting such approvals within three Business Days of a request from the Service Provider therefor and provided that the current WTS process for requesting approval of equipment changes at Regional Network Centre sites is set out in Appendix F (*Data Centre Infrastructure Capacity Request/Approval Process*).	R	
Request approval from the Province of planned WTS Remote Sites Equipment changes (adds, moves, changes, and deletes) utilizing the Province's current process therefor.		R

Responsibility	Province	Service Provider
Approve or reject Service Provider requests for planned equipment changes at each WTS Remote Site within 2 Business Days of Service Provider's request for approval in accordance with the criteria identified by the Province.	R	
In connection with the Services being provided for the WTS Remote Sites Equipment, request adds, moves, changes, and deletes of power outlets, LAN ports, VLAN configuration changes, IP addressing, routing, ACL, structured cabling, cable trays, server enclosures, rack power bars, and seismic restraining to be provided by the Province at WTS Remote Sites.		R
Approve or reject requests of the Service Provider for adds, moves, changes, and deletes of power outlets, LAN ports, VLAN configuration changes, IP addressing, routing, ACL, structured cabling, cable trays, server enclosures, rack power bars, and seismic restraining at WTS Remote Sites within three Business Days of the request and based on the criteria for such adds, moves, changes and deletes of which the Province has given Service Provider notice.	R	
Perform adds, moves, changes, and deletes of power outlets, structured cabling, cable trays, server enclosures, rack power bars, and seismic restraining at WTS Remote Sites in accordance with requests of the Service Provider that have been approved by the Province within 2 weeks of the request.	R	
Provide all requested LAN ports, VLAN configuration changes, IP addressing, routing, ACL in accordance with requests of the Service Provider that have been approved by the Province within 2 weeks of the request.	R	
Supply, manage and support all network hardware, network software, and network configurations within the WTS Remote Sites (other than as provided by the Service Provider in Part IV (*Network Services*) of the Data Centre Services SOW) as required by the applications operating on the WTS Remote Sites Equipment and to enable the Service Provider to communicate with and support the WTS Remote Sites Equipment as part of the Managed Services.	R	

Responsibility	Province	Service Provider
Monitor network capacity of LAN, router, and firewall infrastructure components within the WTS Remote Sites and supply, install and support new network hardware such as routers, switches and firewalls when additional port, bandwidth or firewall capacity is required by the applications operating on the WTS Remote Sites Equipment and to enable the Service Provider to communicate with and support the WTS Remote Sites Equipment as part of the Managed Services.	R	
Monitor network performance within the WTS Remote Sites and upgrade network components such as routers, switches, firewalls, network cabling and carrier lines when additional performance and/or speed is required by the applications operating on the WTS Remote Sites Equipment and to enable the Service Provider to communicate with and support the WTS Remote Sites Equipment as part of the Managed Services.	R	
Refresh the network hardware and software provided by the Province at the WTS Remote Sites when it reaches the end of its asset life or when the hardware / software is no longer supported by a maintenance agreement.	R	
Notify Service Provider of any network maintenance or upgrade event that impacts or could potentially impact the WTS Remote Sites Equipment or the ability of the Service Provider to perform the Managed Services for such WTS Remote Sites Equipment.	R	
Upon request by the Service Provider, provide such network capacity and network performance reports as are available within 5 Business Days of the Service Provider's request. (The reports will be used to help diagnose issues and/or problems with the Service supplied by the Service Provider.)	R	
Provide and install patch cords between WTS Remote Sites Equipment and LAN ports provided by the Province.		R
Notify Province of any MAC address change relating to the WTS Remote Sites Equipment that occurs within the WTS Remote Site.		R
Where it is not reasonably possible for the Province to accept delivery and securely store the WTS Remote Sites Equipment, transport the WTS Remote Sites Equipment to the WTS Remote Sites for installation.		R
Provide access to garbage and recycling facilities for disposal of packing material at each WTS Remote Site.	R	

Responsibility	Province	Service Provider
For any WTS Remote Sites Equipment brought to a WTS Remote Site by the Service Provider, remove packing material from the WTS Remote Site or dispose of packing material in garbage and recycling facilities at the WTS Remote Site provided by the Province.		R
Review power, cooling air flow and cabling installation of WTS Remote Sites Equipment performed by Service Provider at each WTS Remote Site and notify Service Provider of any corrections in such installations required to remedy deficiencies.	R	
Remedy any WTS Remote Sites Equipment installation deficiencies with regards to power, cooling air flow and cabling of which Service Provider is notified by the Province.		R
For each WTS Remote Site, once all WTS Remote Sites Equipment has been removed, notify the Province network group, through an ITIMS order that all the WTS Remote Sites Equipment has been removed.		R
Remove Service Provider access privileges to each WTS Remote Site as requested. This should be completed within 5 Business Days of the request.	R	

IV. NETWORK SERVICES

This Part IV of the Data Centre Services SOW identities the network services to be provided by the Service Provider in connection with the Service Provider's use of data centre facilities and remote sites for the delivery of Managed Services.

This Part IV of the Data Centre Services SOW is divided into two additional sections:

(i) Section 1 of this Part IV of the Data Centre Services SOW provides an introduction to the network services; and

(ii) Section 2 of this Part IV of the Data Centre Services SOW describes the services to be provided for the network.

1. Introduction

1.1 Sites

The network services will be provided at the Province Designated Network Locations and the STMS Data Centres.

1.2 Effective Date and Term

This Part IV of the Data Centre Services SOW will be effective until such time (the "**Service Provider Network Equipment End Date**") as all routers or other communications equipment of

the Service Provider installed at the Province Designated Network Locations and the STMS Data Centres are removed by the Service Provider.

1.3 Related SOWs or Schedules

1.3.1 Business Continuity/Disaster Recovery

The business continuity and disaster recovery services to be provided by the Service Provider for the services that the Service Provider is providing under this Part IV of the Data Centre Services SOW are described in the *Business Continuity and Disaster Recovery Services SOW*.

2. Network Services

The Service Provider and the Province will implement network solutions to support network connectivity between the Province Network and Service Provider Support Locations. The network solution will be implemented in the following three phases:

(i) Phase one covering the period from Hand-Over Date through the expiration or termination of the Managed Services to:
   a. Enable the Service Provider to remotely manage and support the Managed Equipment located at the Existing WTS Data Centres and at the WTS Remote Sites;

(ii) Phase two covering the period from the Availability Date of the STMS Calgary Data Centre through the expiration or termination of the Managed Services to:
   a. Enable the Service Provider to remotely manage and support the Managed Equipment located at the STMS Calgary Data Centre; and
   b. Enable the Province to utilize the Managed Equipment located at the STMS Calgary Data Centre; and

(iii) Phase three covering the period from the Availability Date of the STMS Interior Data Centre through the expiration or termination of the Managed Services to:
   a. Enable the Service Provider to remotely manage and support the Managed Equipment located at the STMS Interior Data Centre; and
   b. Enable the Province to utilize the Managed Equipment located at the STMS Interior Data Centre.

This solution will support any Broader Public Sector organization that resides on the Province Network and elects to obtain Managed Services from the Service Provider.

Broader Public Sector organizations not obtaining Managed Services from the Service Provider will provide their own network solution into the STMS Data Centres.

2.1 Phase One

For phase one, the Province will provide:

- the Third Party Gateways for Service Provider network access to the Province Network enabling remote management and support of the Managed Equipment;
- WAN services for the Province Network;

- Service Provider network access to all required WTS Data Centres Equipment and WTS Remote Sites Equipment;
- LAN services as identified in Part II (*Existing WTS Data Centres Services*) of the Data Centre Services SOW for the Existing WTS Data Centres; and
- LAN services as identified in Part III (*WTS Remote Sites Services*) of the Data Centre Services SOW for the WTS Remote Sites.

For phase one, the Service Provider will provide:

- Routers at the Province Network hubs located at the Province Designated Network Locations as the terminating network appliances for the Service Provider's Management Network circuits (the "**Service Provider Network Equipment**"). The Service Provider Network Equipment will be installed at these two locations on the Service Provider side of the demarcation point of the Province's Third Party Gateway;
- Maintenance, monitoring and management of Service Provider Network Equipment at the Province Designated Network Locations; and
- Carrier circuits between the Service Provider's Service Locations and the Service Provider Network Equipment installed at the Province Designated Network Locations to enable the Service Provider to communicate with and manage the Managed Equipment in the Province locations.

The network connectivity for Managed Services during phase one as shown in the following diagram depicts the circuits the Service Provider is responsible for implementing by the green circuit lines labeled with an A1 through A6.

S15

2.2 Phase Two

For phase two, the Province will provide:

- S. 15

  S. 15 to support:

  (i) the needs of the Transformation Plan (migration of servers and storage to the STMS Calgary Data Centre);
  (ii) remote management and support of the Managed Equipment at the STMS Calgary Data Centre; and
  (iii) Province user access to the applications hosted on the Managed Equipment at the STMS Calgary Data Centre.

For phase two, the Service Provider will provide:

- Routers at the STMS Calgary Data Centre as the terminating network appliances for access to the Service Provider Managed Services for the Province supplied circuits;
- Router upgrades to the Service Provider supplied routers at the Province Network hubs located at the Province Designated Network Locations to extend the routers as the terminating network appliances for the Province supplied circuits;
- Internal network configurations within the Customer Environment for the Province at the STMS Calgary Data Centre consisting of firewalls, intrusion prevention system ("**IPS**") devices, and LAN switches as more fully described in the Security SOW;
- S. 15

  S. 15 ; and
- Maintenance, monitoring and management of Service Provider Network Equipment at the STMS Calgary Data Centre.

The network connectivity for Managed Services during phase two as shown in the following diagram depicts the circuits the Province is responsible for ordering by the blue circuit lines labeled with a B1a and B1b. The Service Provider will be responsible for managing the Province supplied circuits labeled as B1a and B1b. Additionally, during phase two the Service Provider add the circuit identified as C1 in the drawing and begin leveraging the circuit identified as A7 in the drawing.

S15

2.3 Phase Three

For phase three, the Province will provide:

S15

For phase three, the Service Provider will provide:

- Routers at the STMS Interior Data Centre as the terminating network appliances for access to Service Provider Managed Services for the Province supplied circuits;
- Router upgrades/changes to the Service Provider supplied routers at the Province Network hubs located at the Province Designated Network Locations to extend the routers as the terminating network appliances for the Province supplied circuits;
- Internal network configurations within the Customer Environment for the Province at the STMS Interior Data Centre consisting of firewalls, IPS devices, and LAN switches as more fully described in the Security SOW; and
- Maintenance, monitoring and management of Service Provider Network Equipment at the STMS Interior Data Centre.

The network connectivity for Managed Services during phase three as shown in the following diagram depicts the circuits the Province is responsible for ordering by the blue circuit lines labeled with B1 through B4. The Service Provider will be responsible for managing the Province supplied circuits labeled with B1 through B4. The B1a and B1b circuits as identified in Section 2.2 (*Phase Two*) of the Data Centre Services SOW will be upgraded and / or decommissioned as circuits B1 through B4 are activated, but there may be an overlap up to 3 months where all or a portion of all circuits will be active.

The circuits provided by the Province will be provisioned with adequate capacity, estimated at 10Gbps for phase three, to support:

(i) the needs of the Transformation Plan (migration of servers and storage to the STMS Data Centres);
(ii) remote management and support of the Managed Equipment at the STMS Data Centres;
(iii) Province user access to the applications hosted on the Managed Equipment at the STMS Data Centres;
(iv) redundant Province user access to the applications hosted on the Managed Equipment at the STMS Data Centres; and
(v) remote backup and recovery, data replication, data archiving, and other high availability options required between the STMS Data Centres in support of Managed Services.

S15

2.4 Network Services Responsibilities

The responsibilities of the network services are defined below:

Responsibility	Province	Service Provider
Designate a representative who will be authorized to act as Province's primary contact for Service Provider in dealing with the Service Provider Network Equipment to be provided by the Service Provider and located at Province Designated Network Locations and who will have the authority to make decisions on behalf of Province about actions to be taken by Service Provider.	R	
Provision the Service Provider Network Equipment at the S. 15 Province Designated Network Locations to implement network connectivity to enable the Service Provider to communicate with and manage the WTS Data Centres Equipment and the WTS Remote Sites Equipment as part of the Managed Services.		R
Provide equipment racks and power at the Province Designated Network Locations where the Service Provider Network Equipment will be located.	R	
Assign internet protocol ("**IP**") address range(s) for the Service Provider Network Equipment.	R	
Perform initial design, engineering, device staging, and implementation of Service Provider Network Equipment at the Province Designated Network Locations.		R
Provide carrier communication lines required between the Service Provider Support Locations and the Service Provider Network Equipment at the Province Designated Network Locations.		R
Allow Service Provider network traffic to traverse SPAN/BC from/to the Service Provider Network Equipment at the Province Designated Network Locations and the Managed Equipment to support the monitoring and management of such equipment.	R	
Provide remote monitoring and management of Service Provider Network Equipment on a 24 x 7 basis.		R
Provide support and maintenance for Service Provider Network Equipment.		R
Provide reporting on Service Provider Network Equipment performance in accordance with Section B.2.1 of Appendix B (*Reports*).		R
Provide and manage the Third Party Gateway and the network connectivity from the Service Provider Network Equipment to the Managed Equipment at the Existing WTS Data Centres and at the WTS Remote Sites.	R	
Provide circuits as identified in sections 2.2 (B1a and B1b) and 2.3 (B1, B2, B3, B4) of this Part IV of the Data Centre Services SOW.	R	

V. STMS DATA CENTRE SERVICES

This Part V of the Data Centre Services SOW describes, in detail, the scope and functions of the STMS Data Centres provided by the Service Provider. It is divided into five additional sections:

(i) Section 1 provides an introduction to the services;
(ii) Section 2 describes features of the data centres from which the data centre services will be provided and which features represent integral components of such data centre services (the "**Common Data Centre Features**");
(iii) Section 3 describes the core data centre services (referred to, together with the Common Data Centre Features, as the "**Core STMS Data Centre Services**");
(iv) Section 4 describes data centre services that are available on an optional basis (referred to, together with the Common Data Centre Features, as the "**Optional STMS Data Centre Services**"); and
(v) Section 5 sets out certain additional terms and conditions that apply to the Core STMS Data Centre Services and the Optional STMS Data Centre Services ("**Other Terms**").

The Core STMS Data Centre Services and the Optional STMS Data Centre Services are referred to collectively as the "**STMS Data Centre Services**".

1. Introduction

1.1 Sites

The STMS Data Centres Services will be provided from the data centre facilities identified in Part V of Appendix E (*Service Provider Service Locations*).

The size of each of the STMS Data Centres is described in Part V of Appendix E (*Service Provider Service Locations*) of this SOW. The available capacity of each of the STMS Data Centres is based, in part, on the Province VA Commitment to Volt-Amps (or **VAs**) over the Term of the Agreement, as described in Schedule 23 of the Agreement. The STMS Data Centres will have additional capacity in VAs for services to commercial clients and will provide VA capacity growth for the Province all as described in and limited by Schedule 23 of the Agreement.

1.2 Effective Date and Term

This Part V of the Data Centre Services SOW will be effective with respect to each STMS Data Centre, commencing on the Availability Date (except as otherwise indicated expressly to the contrary in this Part V of the Data Centre Services SOW) and, subject to the terms of the Agreement, continuing throughout the Term of the Agreement.

1.3 Managed Services and Co-Location Services

The STMS Data Centre Services described in this Part V of the Data Centre Services SOW are used in two ways:

(i) by the Service Provider in providing Managed Services to the Province (the "**Managed Services Customer**" or "**MSC**"); and

(ii) as "co-location services" by Buyers ("**Co-location Customers**") in connection with the operations of their information technology infrastructure. For the purposes of this document, if the Province ceases to obtain Managed Services from the Service Provider during the Data Centre Services Term of the Agreement, then the Province will be considered a Co-location Customer.

The Service Provider, in using the STMS Data Centre Services to provide Managed Services, and the Co-location Customers in their use of the STMS Data Centre Services, will operate within one or more secure co-location Cages or cabinets on the raised floor area of the STMS Data Centre, as more completely described below.

With respect to the STMS Data Centre Services, the interactions between the Service Provider and Province differ from the interactions between the Service Provider and Co-location Customers. To capture the differences, the RASIC tables in this Part V of the Data Centre Services SOW contain separate column groups for Managed Services (the "Managed" column group) and for "co-location services" (the "Co-location" column group). If the Province ceases to obtain Managed Services from the Service Provider, then the Province will revert to Co-location Customers and be responsible for the performance of the Co-location Customer's responsibilities set out in this Part V of the Data Centre Services SOW during such remaining period of time as this Part V of the Data Centre Services SOW continues in effect.

The Co-location Customers will purchase the STMS Data Centre Services through the Service Provider with each Co-location Customer entering into a separate agreement with the Service Provider and being treated as a separate Customer. Accordingly, each Co-location Customer will have its own access and visibility, including without limitation, the Q9 Control Panel into its environment and may interact directly with Service Provider staff for operational issues related to the co-location environment. Billing and administrative issues with respect to the Co-location Customers will be coordinated by Service Provider.

In this Part V of the Data Centre Services SOW:

(i) "**Customer Environment**" means for the Managed Services Customer or for each Co-location Customers or for each Broader Public Sector entities that purchase Managed Services from the Service Provider, the Cage(s) constructed by Service Provider for delivering Managed Services, or for Co-location Customers or for Broader Public Sector entities that purchase Managed Services from the Service Provider, including Q9-Cabinet(s), if such cabinets are provided. For greater clarification, a Customer Environment may be just a Q9-Cabinet without a Cage; and

(ii) "**Environment Controller**" means the organization (Service Provider in the case of Managed Services, or Co-location Customer in connection with the "co-location services") that is in control of the Customer Environment used in the provision of STMS Data Centre Services.

1.4 Related SOWs or Schedules

1.4.1 Service Levels

The Service Levels applicable to the STMS Data Centre Services are described in Schedules 11 to the Agreement.

1.4.2 Business Continuity/Disaster Recovery

Business continuity and disaster recovery in respect of the STMS Data Centre Services used in providing the Managed Services are described in the *Business Continuity and Disaster Recovery Services SOW*.

Co-location Customers will have access to the services described in the Services Catalogue for building business continuity and disaster recovery services.

2. Common Data Centre Features

This section describes features of the STMS Data Centres from which the STMS Data Centre Services will be provided.

The charges for the Common Data Centre Features are not separately identified but are included within the monthly fees charged for the Capacity Reservation.

2.1 Physical Security

Physical security will be provided at and within each STMS Data Centre as follows:

S15

S15

In accordance with the foregoing, Co-location Customers will have 7 x 24 unannounced access privileges to their Customer Environment at the STMS Data Centres. Access by the Province to the Customer Environment of the Province at the STMS Data Centres will be coordinated through the Service Provider. The Province will notify the Service Provider of individuals who may authorize Province access to the Customer Environment of the Province at the STMS Data Centres through the Governance Procedures described in the Agreement.

A Co-location Customer will be notified where there has been access to its Customer Environment other than in accordance with the existing access control procedures in effect at the STMS Data Centre or it is reasonably likely that such access to its Customer Environment may have occurred.

Physical security incidents will be investigated upon written request from the Province or Co-location Customer of a serious incident at an STMS Data Centre (including reviewing available

archived video footage). Service Provider will report to the Province or the Co-location Customer on the results of the investigation including providing any relevant portions of video footage (edited to protect the privacy of other customers).

2.2 Power Systems

Power systems will be installed and maintained within each STMS Data Centre as follows:

(i) The power distribution system design will not preclude future support for two high-voltage utility feeds for the STMS Data Centre (regardless of whether, at the time the data centre is built, two high-voltage utility feeds are available at the data centre on reasonable terms from the local utility power supplier or suppliers);

(ii) Other than in respect of the high-voltage utility feeds, the power distribution systems at the STMS Data Centres will be built to a minimum of N+1 Redundancy:

(a) Multiple UPS systems will provide conditioned power to Environment Controller Provided Equipment in each STMS Data Centre. The combined UPS systems in each STMS Data Centre will, at a minimum, be capable of supporting the data centre at 100% of the STMS Data Centre design capacity;

(b) A system of N+1 Redundancy power generators at each STMS Data Centre will be designed to provide power to the STMS Data Centre when required as a result of issues with the quality or availability of local utility power. The generator system at each STMS Data Centre will, at a minimum, be capable of supporting the data centre at 100% of the STMS Data Centre design capacity; and

(c) The power systems within each STMS Data Centre are designed to enable all routine maintenance of the power systems to be conducted without interruption of service (recognizing that redundancy levels may be impacted during such maintenance);

(iii) Sufficient generator fuel will be maintained onsite at each STMS Data Centre to support power generation for at least S15 following a utility power quality or availability event at 100% of the STMS Data Centre Total Contracted Capacity;

(iv) Diesel fuel delivery arrangements will be maintained with multiple suppliers. Subject to the availability of diesel fuel, the STMS Data Centres are designed to operate indefinitely in the event of a prolonged disruption of utility power;

(v) Power will be delivered to each Environment Controller rack in each STMS Data Centre using at least two independent power sources (unless requested otherwise by the Environment Controller); and

(vi) A continuous test program for the power systems will be maintained at each STMS Data Centre that will test the emergency standby power systems at the data centre at least once each calendar month.

Environment Controllers will be notified at an STMS Data Centre where an event affecting the power systems at the data centre will impact the Environment Controller, including without limitation, any Service Levels. Notice will be given in accordance with the Environment Controller's emergency escalation list as prescribed in the Q9 Control Panel. The events affecting power systems where notice will be provided include where one of the redundant power sources has been or will be unavailable (but not including situations where one of the power sources that is provided to the rack or cabinet during maintenance is raw power that is not protected by UPS or generator systems).

Environment Controllers who wish to take full advantage of the two independent power sources at the STMS Data Centres must implement equipment with dual power supplies (equipment capable of drawing power from either power supply or both power supplies).

Environment Controllers will only utilize the power made available to their Customer Environment in accordance with the policies and procedures for power systems provided through the Q9 Control Panel and in accordance with section 5.3 (*Exceeding Capacity Reservation*) of this Part V of the Data Centre Services SOW.

2.3 Fire Systems

Fire detection and prevention systems will be implemented at each STMS Data Centre as follows:

(i) each STMS Data Centre will be equipped at a minimum with a VESDA® (Very Early Smoke Detection Apparatus) smoke detection system or alternate smoke detection system providing equivalent functionality;

(ii) the fire detection systems at each STMS Data Centre will be linked to the data centre monitoring and alert subsystems in order to notify data centre staff of the need to investigate an alert or a potential fire incident in the data centre;

(iii) each STMS Data Centre will be equipped with a zoned dry-pipe, pre-action sprinkler system (in accordance with NFPA-75);

(iv) clean agent fire suppression systems will be deployed at such locations within the STMS Data Centre as are determined by Service Provider, considering the floor plan of the STMS Data Centre; and

(v) manual fire extinguishers will be located throughout each STMS Data Centre.

Appropriate personnel at each STMS Data Centre will be provided with written procedures and contact information for monitoring, handling and escalating alerts from the fire detection systems.

The systems in effect at each STMS Data Centre will not automatically shut off power to a Customer Environment when pre-action sprinkler systems are activated in the data centre.

2.4 Environmental Systems

Environmental systems (i.e. building systems for heating, cooling and humidification) will be installed and maintained at each STMS Data Centre as follows:

(i) Environmental systems will be implemented at each STMS Data Centre that incorporate a minimum of N+1 Redundancy and permit all routine maintenance to be conducted without interruption of service (recognizing that redundancy levels may be impacted during such maintenance). These environmental systems are either in continuous operation, cycled from standby to duty use at least once each calendar month or tested at least once each calendar month;

(ii) The environmental systems at each STMS Data Centre will be capable of supporting the data centre at 100% of the STMS Data Centre design capacity;

(iii) The environmental systems implemented at each STMS Data Centre will utilize a cooling system that does not rely on municipal water supply services or base building water supplies for primary cooling; and

(iv) The design at each STMS Data Centre will be capable of providing, at a minimum effective cooling for Environment Controller Provided Equipment in the data centre that consumes an average of 100 watts per square foot.

Environment Controllers will locate equipment in their Customer Environment so as not to exceed the cooling capacity provided by the environmental systems in each STMS Data Centre. The Co-location Customer will advise Service Provider if the Co-location Customer anticipates or recognizes that equipment densities in the Customer Environment will require a greater cooling capacity, i.e. in excess of 100 watts per square foot and Co-location Customer may also be notified if such cooling capacity is being exceeded. In such event, written cooling distribution recommendations for such higher equipment densities will be developed for the Co-location Customers and such recommendations will be implemented by the Co-location Customers.

If the equipment densities in a Customer Environment exceed such environment's cooling capacity and either impact the environments of other STMS Data Centre customers or the STMS Data Centre itself, then the Co-location Customers may be required to shut down Environment Controller Provided Equipment or Service Provider may shut off that portion of the power supply services required to alleviate the impact on the environments of other customer or the STMS Data Centre itself, all in accordance with section 5.3 (*Exceeding Capacity Reservation*) of this Part V of the Data Centre Services SOW.

2.5 Onsite Amenities

Each STMS Data Centre will include common amenities described below for the use of all customers of the data centre outside the Customer Environment Area at the data centre. Use of these amenities will be shared among customers of the data centre on an "as available" basis.

The following Onsite Amenities are generally not considered critical to customer operations and may be delayed by a few weeks/months after the Availability Date of each STMS Data Centre:

- On-site work area;
- Conference meeting rooms;

- Reception area;
- Day-use lockers;
- Small lunch room.

2.5.1 On-site work space for Visitors

Access to shared office space for at least 4 Visitors will be provided at each STMS Data Centre for the use, as and when available, by all customers, such office space to include power, public Internet access and Public Switched Telephone Network ("**PSTN**") access.

2.5.2 Conference Meeting Rooms

At least two conference meeting rooms will be provided at each STMS Data Centre. Each conference room will be equipped with power, a single PSTN access, and a public Internet connection and be suitable for meetings with up to eight individuals. Environment Controllers will be able to reserve a conference room (on an "as available" basis) for onsite meetings. Service Provider will manage the conference room booking procedure at each STMS Data Centre and the booking procedure will be described in the Q9 Customer Guide found on the Q9 Control Panel.

2.5.3 Reception Area

A reception area will be provided and maintained at each STMS Data Centre for Visitors to meet before entering the raised floor area.

2.5.4 Staging Area

A staging area outside of the Customer Environment Area will be provided at each STMS Data Centre for unpacking equipment prior to moving it into the Customer Environment Area. The staging area will not be a secure area and equipment should not be left or stored in this area of the data centre. (Any equipment left or stored in the staging area by the Environment Controller will be at the Environment Controller's risk.)

Access will be provided to garbage and recycling facilities for disposal of packing material at each STMS Data Centre. Environment Controllers must remove packing material from the staging area or dispose of packing material in the provided garbage and recycling facilities.

A dolly will be provided, on a shared and "as available" basis, in the equipment staging area.

2.5.5 Secure Temporary Storage Area

A secure storage area for the short-term (i.e. up to 24 hours) storage of Environment Controller Provider Equipment that has been delivered or shipped to the STMS Data Centre will be provided at each STMS Data Centre. The secure temporary storage area will be outside the Customer Environment Area. Environment Controllers will be provided with access to the secure temporary storage area. A dolly will be provided, on a shared and "as available" basis, in the secure temporary storage area. Equipment left in such storage area will be considered Environment Controller Provider Equipment.

Environment Controllers are required to remove equipment from the secure temporary storage area within 24 hours.

A secure storage service will be provided in the Service Catalogue for medium-term (i.e. weekly) storage of equipment on a temporary basis.

2.5.6 Visitor Amenities

The following amenities will be provided for data centre visitors at each STMS Data Centre outside the Customer Environment Area:

(i) Day-use lockers suitable for small items carried by visitors (such as coats, boots, bags, etc.);
(ii) Small lunch room including lunch room furniture and basic lunch room supplies (i.e. paper towels, sink, water supply and dish/utensil washing soap); and
(iii) Washrooms and washroom supplies.

3. Core STMS Data Centre Services

The Core STMS Data Centre Services consists of the service components described below (together with the Common Data Centre Services).

3.1 Customer Environments

Each Customer Environment is a physically secure environment (i.e. Cage(s) and/or Q9-Cabinet(s)) with biometric access control at an STMS Data Centre.

The Environment Controller will work with Service Provider to define their requirements for their Customer Environment which will be built by Service Provider and installed at the STMS Data Centre. The Environment Controller's requirements will include Capacity Reservation as identified in section 5.2 (*STMS Data Centre Planning*) of this Part V of the Data Centre Services SOW. Pricing for the installation of each Customer Environment will be custom and based on actual requirements. The options available for installation in the Customer Environment and budgetary pricing are set out in the Service Catalogue.

The Environment Controllers may begin working with Service Provider on their Customer Environments in advance of the Availability Date so that the Customer Environment is available on the Availability Date for installation of Environment Controller Provider Equipment. (Environment Controllers who wish to do so should contact Service Provider at least 6 months in advance of the Availability Date to schedule the design of their Customer Environment. In order for the Customer Environment to be available on the Availability Date of the STMS Data Centre, Environment Controllers must approve the design of the Customer Environment no later than 4 months prior to the Availability Date.).

Responsibility	Co-location		Managed	
	Co-location Customer	SP	MSC	SP
Provide specific requirements for each Customer Environment.	R			R

Responsibility	Co-location		Managed	
	Co-location Customer	SP	MSC	SP
Provide written description of each Customer Environment (and Cage diagram where appropriate) that meets each Co-location Customer's or the Province's stated requirements.		R		R
Provide pricing to the Province or Co-location Customer for the installation of and/or changes to the Customer Environment.		R		R
Approve description of Customer Environment (and Cage diagram if applicable) and pricing.	A		A	
Install power circuits and cooling to meet Environment Controller requirements in accordance with approved description of the Customer Environment.		R		R
Install secure Cage(s) and/or Q9-Cabinet(s) in accordance with approved description of Customer Environment.		R		R
Install racks or Environment Controller Provider Enclosures within Cage in accordance with approved description of Customer Environment.		R		
Install cable trays in accordance with approved description of Customer Environment.		R		
Install cabling between racks within Cage(s) where the Environment Controller elects to be responsible for their own cabling in accordance with approved description of Customer Environment.	R	I		R
Install cabling between racks within Cage(s) where the Environment Controller has elected to have Service Provider install the cabling in accordance with approved description of Customer Environment.	C	R		R
Install cabling between Q9-Cabinets in accordance with approved description of Customer Environment.	C	R		R
Install cabling within Environment Controller cabinets and within racks within a Cage.	R			R
Enable reporting of each Environment Controller's aggregate and circuit-level power monitoring on the Q9 Control Panel.		R		R
Physical installation and maintenance of Environment Controller Provider Equipment in Customer Environment.	R			R
Maintain inventory of and insurance for Environment Controller Provider Equipment within each Customer Environment.	R			R
Review power demand reporting for each Customer Environment to coordinate compliance with power redundancy and power demand commitments.	R			R
Monitor cooling (temperature and humidity) within each Customer Environment.	R			R
Distribute equipment evenly throughout the Customer Environment and/or in accordance with Service Provider-provided cooling distribution recommendations.	R	C		R

3.2 Q9 Control Panel

The Q9 Control Panel is a customer portal that provides access to the following services:

- General account management including administration of customer contacts, security access and emergency escalation procedures
- Online access to Q9 Customer Guide including data centre policies and procedures (see section 5.1 (*Data Centre Policies and Procedures*))
- Power monitoring – The Q9 Power Monitoring and Reporting Service provides customers with reports (available online or for export in CSV format) that summarize their current and aggregate peak power demand in each STMS Data Centre. These reports can be used by Environment Controllers to:
  - assist in compliance with their Capacity Reservation;
  - provide for even distribution of power demand throughout their Customer Environment to effectively cool Environment Controller Provider Equipment;
  - confirm that they are within the redundant capacity of the power circuits in their racks and/or cabinets, and;
  - Track their current and historical power demand for capacity planning purposes.
- Creation and management of support tickets
- The following items will also be available in the Q9 Control Panel where the Co-location Customer has ordered the associated services from the Service Catalogue:
  - Network bandwidth reports that display bandwidth utilization in 5-minute averages and the 95th percentile highlighted to give a clear indication of usage for the current month. Additional weekly, monthly and yearly graphs chart historical utilization;
  - Network bandwidth monitoring with customizable threshold alarms;
  - Network status reports;
  - Protocol monitoring (customer-configured monitoring for PING, HTTP, FTP, SMTP, POP3) with automatic issue notification; and
  - Self-administration of customer domains.

The features of Q9 Control Panel are included in the monthly fee charged for Capacity Reservation.

The Service Provider will administer any access authorizations to: (i) the Q9 Control Panel and (ii) the Customer Environment used to provide Managed Services at each STMS Data Centre.

Co-location Customer will be granted access to the Q9 Control Panel in respect of the STMS Data Centre Services being provided to the Co-location Customer. Each Co-location Customer will administer any access authorizations to: (i) the Q9 Control Panel; and (ii) its Customer Environment. However only the Service Provider will be provided with access to the billing information with respect to each Co-location Customer on the Q9 Control Panel. The Service Provider will also be provided with access to the reporting available through the Control Panel for each Co-location Customer.

Responsibility	Co-location		Managed	
	Co-location Customer	SP	MSC	SP
Update each Environment Controller with respect to changes to functionality of the Q9 Control Panel.		R		
Provide Service Provider with the identity of Co-location Customer's primary contact for administering access to the Control Panel and STMS Data Centres.	R			
Update Q9 Control Panel with Co-location Customer's primary contact for administering access to the Control Panel and STMS Data Centres.		R		
Maintain Q9 Control Panel for use on a 7x24 basis.		R		R

3.3 On-site Support

At a minimum, an average of two data centre technicians will be maintained onsite at each STMS Data Centre on a 7x24 basis and at least one data-centre technician onsite at each STMS Data Centre at all times. The data centre technicians will provide the Hands and Eyes service in each STMS Data Centre. "Hands & Eyes" service is an on-site emergency assistance service available to all STMS Data Centre customers on a 7x24 basis in the STMS Data Centres, as described in the Service Catalogue. (Hands and Eyes service is intended for emergency or urgent nonrecurring events only and is not intended for events of a recurring nature such as scheduled backup tape rotations or regular hardware and software maintenance.)

The On-Site Support provided by data centre technicians in included in the monthly fee charged for Capacity Reservation.

Responsibility	Co-location		Managed	
	Co-location Customer	SP	MSC	SP
"Hands & Eyes" service by opening a ticket through the Q9 Control Panel or by calling the Q9 Control Centre.	R	S		R
Provide 7x24 onsite data centre technician to support "Hands & Eyes" service.		R		R
Provide updated list of services available as part of Hands and Eyes service as additions or changes are made.		R		R
Update the Service Catalogue to reflect additions or changes to services available as part of Hands and Eyes service. (Any updates to the Hands and Eyes service will be implemented through the Change Order Process.)		R		R

3.4 Advisory Support Service

Initial and ongoing technical guidance will be provided to Co-location Customers in respect of their Customer Environment in each STMS Data Centre including:

- Assistance with estimating Co-location Customer's current and future data centre capacity requirements;
- Designing a physical space solution that meets each Co-location Customer's requirements;
- Providing each Co-location Customer with an orientation of its STMS Data Centre(s) and the Q9 Control Panel; and
- Reviewing each Customer Environment and educating Co-location Customers about taking advantage of the high-availability power and cooling infrastructure at the STMS Data Centre.

The advisory support services are included in the monthly fee charged for the Capacity Reservation. The advisory support services will be provided by the solutions architect assigned to each Co-location Customer on the Q9 Control Panel. The solutions architect can be scheduled for consultation from 9:00 a.m. to 5:00 p.m. (local time at each STMS Data Centre) on Business Days to provide support to customers at the STMS Data Centre.

	Co-location		Managed	
Responsibility	Co-location Customer	SP	MSC	SP
Request advisory support services by calling or emailing the solutions architect as assigned to the Co-location Customer on the Q9 Control Panel.	R			
Provide technical guidance to Co-location Customers in respect of their Customer Environment in each STMS Data Centre.		R		

4. Optional STMS Data Centre Services

The Service Provider will make available to Co-location Customers Optional STMS Data Centre Services at the STMS Data Centres including:

- Cross-connect services, i.e. services that provide interconnections between a Customer Environment and another environment in the STMS Data Centre, using the data centre's pre-built cross-connect infrastructure (cross-connect services between separate Customer Environments in an STMS Data Centre cannot be provided by Co-location Customers and must be provided by the Service Provider);
- Cabling services within a Customer Environment (to the extent not performed by the Co-location Customer);
- Media destruction services;
- IT equipment disposal services;
- Optional Bandwidth services;
- Managed firewall services;
- Managed load balancer services;
- Managed network device services; and
- Managed remote link services.

The complete list and description of available Optional STMS Data Centre Services together with pricing is set out in the Services Catalogue.

Responsibility	Co-location		Managed	
	Co-location Customer	SP	MSC	SP
Provide updates to the Service Catalogue describing updates or changes to the available optional services. (Any updates to the Service Catalogue will be implemented through the Change Order Process.)		R		
Submit Change Order to request optional services with respect to the Customer Environment	R	S		R
Provide optional services with respect to the Customer Environment as specified in the agreed to Change Order.		R		R

5. *Other Terms*

This Section sets out other provisions applicable to the STMS Data Centre Services.

5.1 Data Centre Policies and Procedures

This section refers to the policies and procedures that will be implemented at the STMS Data Centres together with the responsibilities of the Province, the Service Provider, and Co-location Customers relating to such policies and procedures.

The policies and procedures established for Environment Controller operations in the STMS Data Centres will be described in the Q9 Customer Guide available on the Q9 Control Panel and in written notices provided to the Environment Controllers. The policies and procedures described in the Q9 Customer Guide include the following:

- Procedures for shipping Environment Controller Provider Equipment to the STMS Data Centres;
- Procedures for the removal of Environment Controller Provider Equipment from an STMS Data Centre;
- Requirements for the Environment Controller Provider Equipment and Customer Environment in an STMS Data Centre;
- Procedures for the utilization of power in Customer Environments;
- Access procedures for onsite access to the STMS Data Centres and each Customer Environment;
- Policies for the use of onsite amenities (such as booking conference meeting rooms, use of the shared workspace, use of the staging area, and use of on-site recycling bins); and
- Procedures for Environment Controller communications (such as opening tickets and notification of service impacting events).

The policies and procedures established for Co-location Customers operations in the STMS Data Centre will be updated from time to time during the Term of the Agreement. Co-location Customers will be advised, through e-mail to the Co-location Customers contact recorded on the

Q9 Control Panel, of updates to the policies and procedures in effect at an STMS Data Centre including the effective date of such updates. Updates to such policies and procedures will not:

(i) inhibit access to Customer Environments or Environment Controller Provider Equipment;

(ii) adversely impact or diminish the Services provided from the STMS Data Centres; or

(iii) reduce the support provided to Co-location Customers as described in this Part V of the Data Centre Services SOW and the Service Catalogue.

	Co-location		Managed	
Responsibility	Co-location Customer	SP	MSC	SP
Maintain the currency of data centre processes and procedures contained in the Q9 Control Panel for each STMS Data Centre.		R		R
Identify when a new STMS Data Centre process or procedure needs to be added to the Q9 Control Panel.	S	R		R
Initiate and communicate to Co-location Customers any updates to existing data centre processes and procedures at each STMS Data Centre through the Q9 Control Panel or through separate written notice to the Co-location Customer.		R		

5.2 STMS Data Centre Planning

The Province VA Commitment is an aggregate reservation of VA capacity at the STMS Data Centres. The Province and Buyers may share the Province VA Commitment amongst themselves in such manner as they deem appropriate in accordance with the provisions of the Agreement. The Province and Buyer will each notify the Service Provider of the Capacity Reservation of each Buyer and of any changes to such Capacity Reservation through the Change Order Process.

If the Province or a Buyer desires to increase its Capacity Reservation, as applicable, and

(i) if the STMS Data Centre has VA capacity available to provide such increase, then the Environment Controller must approve the design of its Customer Environment at the time of the Change Order for such increase; or

(ii) if the STMS Data Centre does not then have VA capacity available to provide such increase, then the Co-location Customer should contact the Service Provider at least 6 months in advance of the date the increase VA capacity is expected to become available to schedule the design of the Customer Environment, and must approve the design no later than 4 months prior to such date. In the case of the Province, the Service Provider will design the appropriate Customer Environment.

The Province and Service Provider have agreed to a cooperative planning process with respect to the Province VA Commitment to optimize aggregate usage by Co-location Customers, the Managed Services Customer and any Broader Public Sector that purchase Managed Services

from the Service Provider of the Province VA Commitment at each STMS Data Centre and to implement any adjustments to the Province VA Commitment in an effective manner.

The cooperative planning process agreed to by the Province and the Service Provider involves:

(i) preparation and updating of a three year plan (the "**STMS Data Centres Three Year Plan**"); and

(ii) periodic meetings ("**Periodic Capacity Review Meetings**") to review and discuss capacity requirements and availability at the STMS Data Centres and the STMS Data Centres Three Year Plan.

5.2.1 STMS Data Centres Three Year Plan

Each STMS Data Centres Three Year Plan will report on:

(i) usage of the Province VA Commitment at each STMS Data Centre including, by name of Co-location Customer or Managed Services Customer or Broader Public Sector entity that purchases Managed Services from the Service Provider, VA consumption against predicted usage and the Capacity Reservation and three year projections of future VA requirements;

(ii) Projected VA requirements of entities anticipated to become Buyers in future;

(iii) Three year projections of the available capacity in each STMS Data Centre; and

(iv) Technology changes that are anticipated, in the opinion of the Service Provider, to occur within the following three year period together with the Service Provider's assessment of VA requirements associated with such technology changes.

The first STMS Data Centres Three Year Plan will be prepared by the Service Provider within seven months of the Effective Date. Thereafter, the STMS Data Centres Three Year Plan will be updated by the Service Provider for each Periodic Capacity Review Meeting. The Service Provider will provide a copy of the STMS Data Centres Three Year Plan to the Province ten Business Days prior to the Periodic Capacity Review Meeting.

The STMS Data Centre Three Year Plan will be prepared as part of and in conjunction with the Annual Operating Plans referred to in the Agreement.

In connection with each STMS Data Centres Three Year Plan prepared by the Service Provider:

(i) the Province will be responsible for identifying the potential Capacity Reservations of any Buyers intending to procure services in the future that are not already known to the Service Provider; and

(ii) the Province and each Broader Public Sector entity that purchases Managed Services from the Service Provider, will be responsible for forecasting their systems expected to be added or removed during the period covered by the STMS Data Centres Three Year Plan Due to such entities business requirement; and

(iii) each Co-location Customer will be responsible for providing the Service Provider with information related to its VA usage required to prepare the STMS Data Centres Three Year Plan including VA consumption against predicted usage, three year projections of future VA requirements and anticipated increases or decreases in the Capacity Reservation; and

(iv) the Service Provider will be responsible for
  (a) consolidating the information provided by the Province, any Broader Public Sector entities that purchase Managed Services from the Service Provider and the Co-location Customers for the STMS Data Centres Three Year Plan; and
  (b) projecting any adjustments to the Capacity Reservation or Province VA Commitment based on the Managed Services Customer system projections and system projections from Broader Public Sector that purchase Managed Services from the Service Provider, the information provided by the Co-location Customers and the Service Provider's transformation activities.

5.2.2 Periodic Capacity Review Meetings

The Service Provider will schedule Periodic Capacity Review Meetings with the Province twice annually during the Term of the Agreement no more than seven months apart. The first Periodic Capacity Review Meeting will occur within seven months of the Effective Date.

The purpose of the Periodic Capacity Review Meetings will be to optimize aggregate usage by Co-location Customers, the Managed Services Customer and any Broader Public Sector entities that purchase Managed Services from the Service Provider of the Province VA Commitment at each STMS Data Centre and to consider any adjustments to the Province VA Commitment including adjustments to the phase-in of the Province VA Commitment or Capacity Reservation.

In connection with each Periodic Capacity Review Meeting:

(i) the Province may determine to make no changes to the Province VA Commitment or the Capacity Reservation of any Co-location Customer or Managed Services Customer or any Broader Public Sector that purchase Managed Services from the Service Provider;

(ii) the Province may re-allocate Capacity Reservations at each STMS Data Centre to better match the actual current and anticipated future requirements of Customers without increasing or reducing the Province VA Commitment. The Province will notify the Service Provider of any reallocation of Capacity Reservation amongst Co-location Customers and any Broader Public Sector entities that purchase Managed Services from the Service Provider. Any re-allocation of the Capacity Reservations that requires changes to a Customer Environment will be implemented in accordance with the Change Order Process and may result in one-time implementation charges;

(iii) subject to availability, Co-location Customers, the Managed Services Customer or any Broader Public Sector entities that purchase Managed Services from the Service Provider may request Additional Capacity Reservation in a particular STMS Data Centre in accordance with Schedule 23 (Fees) of the Agreement;

(iv) the Province may reduce the Province VA Commitment at an aggregate level once in each Contract Year in accordance with Schedule 23 (Fees) of the Agreement;

(v) the Province may reduce the Province VA Commitment at an aggregate level on an extraordinary basis in accordance with Schedule 23 (Fees) of the Agreement; and

(vi) subject to availability, the Province may request Additional Capacity Reservation in a particular STMS Data Centre in accordance with Schedule 23 (Fees) of the Agreement.

Changes in the Province VA Commitment impacting the Service Provider including re-allocations of Capacity Reservations that require changes to a Customer Environment will be implemented in accordance with the Change Order Process defined in the Agreement.

The Periodic Capacity Review Meetings will be integrated within the Governance process of this Agreement.

5.2.3 Recommended Increases in Province VA Commitment

The Service Provider may recommend to the Province that the Province increase the Province VA Commitment at either or both STMS Data Centres based on:

(i) the STMS Data Centres Three Year Plan;

(ii) forecasts including planned transformation activities for Managed Services;

(iii) Service Provider monitoring of power demand relating to the Managed Services; or

(iv) Capacity Reservation requirements of Buyers as identified by them;

and subject to available capacity at the STMS Data Centres.

In connection with any recommendation by the Service Provider that the Province increase the Province VA Commitment at an STMS Data Centre, the Service Provider will also identify for the Province the potential consequences of any failure to increase the Province VA Commitment. Any increase in the Province VA Commitment will be implemented in accordance with the Change Order Process set out in the Agreement.

If the Province does not accept the Service Provider's recommendation that the Province increase the Province VA Commitment, then the Province acknowledges that the potential consequences of the failure to increase the Province VA Commitment may include:

(i) the Service Provider may be unable to meet its service provision commitments in response to any individual request by the Province or any Broader Public Sector entities that purchase Managed Services from the Service Provider for additional Servers, storage and backup equipment or network equipment;

(ii) the Service Provider may be unable to proceed with the Transformation Plan for the Province or any Broader Public Sector entities that purchased Managed Services from the Service Provider due to the unavailability of required VA capacity;

(iii) the Service Provider may be unable to install new Service Management Systems required for ongoing Service delivery to the Province or any Broader Public Sector entities that purchase Managed Services from the Service Provider, resulting in Service failures; and

(iv) the inability of the Service Provider to make additional capacity available to Co-location Customers.

5.3 Exceeding Capacity Reservation

Each Co-location Customer is responsible for the VA capacity it requires for its Systems (applications and hardware) located in an STMS Data Centre. In particular, each Co-location Customer is responsible for ensuring that its application and hardware deployment plans include an assessment of whether it has sufficient VAs available under its Capacity Reservation to meet its requirements through:

(i) planning to provide that VA capacity will be available to the Co-Location Customer to meet its future VA requirements;

(ii) monitoring and verification that its current power demand falls within its Capacity Reservation (the Service Provider and Co-location Customers have the ability to monitor power demand on a near real time basis through the Q9 Control Panel); and

(iii) ongoing assessments of the differences between past planning estimates and the Co-location Customer's actual deployment requirements in order to improve future planning.

The Service Provider and the Province have established the capacity planning process set out in Section 5.2 (*STMS Data Centres Planning*) of this Part V of the Data Centre Services SOW to assist the Province, any Broader Public Sector entities that purchase Managed Services from the Service Provider, and the Co-location Customers in planning for any required adjustments to the Province VA Commitment or the Capacity Reservations.

This section sets out the results of any Co-location Customer exceeding its Capacity Reservation in three circumstances.

5.3.1 Co-location Customer exceeds its Capacity Reservation, Province VA Commitment not exceeded.

Subject to section 5.3.4 of this Part V of the Data Centre Services SOW, no action will be taken by the Service Provider. However, a redesign of the Customer Environments may be required in order to accommodate a redistribution of capacity among the Co-location Customers and the Managed Services Customer and any Broader Public Sector entities that purchase Managed Services from the Service Provider. The redesign of the Customer Environments is chargeable and may require an outage in order to relocate equipment to accommodate the redesign of the physical environments.

5.3.2 Co-location Customer exceeds its Capacity Reservation, Province VA Commitment exceeded, STMS Data Centre has available VA Capacity.

Subject to section 5.3.4 of this Part V of the Data Centre Services SOW, the Service Provider will promptly notify Co-location Customer, in accordance with the Co-location Customer's emergency escalation list as prescribed in the Q9 Control Panel, that Co-location Customer has exceeded its Capacity Reservation and the Province that the Province has exceeded the Province VA Commitment.

Within five Business Days of the Service Provider so notifying the Co-location Customer and Province, the Service Provider, the Co-location Customer and the Province will consult and will determine whether to:

(i) request an increase in the Province VA Commitment;

(ii) decrease the Co-location Customer's power demand to be within its Capacity Reservation; or

(iii) combined with (i) and (ii) above and subject to the redesign conditions outlined in section 5.3.1, reallocate the Province VA Commitment allocated among Co-location Customers, the Managed Services Customer and any Broader Public Sector entities that purchase Managed Services from the Service Provider to take advantage of VA capacity reserved for Co-location Customers , the Managed Services Customer and any Broader Public Sector entities that purchase Managed Services from the Service Provider but not currently required by them.

5.3.3 Co-location Customer exceeds its Capacity Reservation, Province VA Commitment exceeded, STMS Data Centre does not have VA Capacity available.

Subject to section 5.3.4 of this Part V of the Data Centre Services SOW, Service Provider will promptly notify Co-location Customer, in accordance with the Co-location Customer's emergency escalation list as prescribed in the Q9 Control Panel, that Co-location Customer has exceeded its Capacity Reservation and the Province that the Province has exceeded its Province VA Commitment and of any determination by Service Provider that the Co-location Customer exceeding its Capacity Reservation and the Province exceeding its Province VA Commitment may result in an impairment of Service Provider's ability to deliver redundant services to other customers within the STMS Data Centre.

Where the notice provided by the Service Provider specifies that it has determined that the Co-location Customer exceeding its Capacity Reservation and the Province exceeding its Province VA Commitment may result in impairment of Service Provider's ability to deliver redundant services to other customers within the STMS Data Centre, then:

(i) the Service Provider will consult with the Province and the Co-location Customer who is exceeding its Capacity Reservation;

(ii) within twelve hours of Service Provider's notice to the Province, the Province will cause the Co-location Customer who is exceeding its Capacity Reservation to decrease its power or will take or direct the Service Provider to take other action as may be required so that the Province VA Commitment is not exceeded;

(iii) if the Service Provider is not able to consult with the Province within twelve hours of Service Provider's notice to the Province, then the Service Provider may take such action as the Service Provider believes is reasonable in the circumstances so that the Province VA Commitment and/or Co-location Customer's Capacity Reservation is not exceeded; and

(iv) if Service Provider, in consultation with the Province and the applicable Co-location Customer, does not decrease the Co-location Customer's power demand below the applicable Capacity Reservation or take other action such that Province VA Commitment is not exceeded within twelve hours of Service Provider's notice to Province, Service Provider may shut off that portion of the power supply services to the Co-location Customer as is required to decrease the Province's demand to a level at or below the Province VA Commitment, provided that Service Provider will only shut off power supply in instances where there arises any hazardous condition, unsafe practice or emergency situation as determined by the Service Provider.

5.3.4 Co-location Customer exceeds its Capacity Reservation and there is a present or imminent impact on ability of Service Provider to deliver services to other customers

If a Co-location Customer exceeds its Capacity Reservation and the Co-location Customer's excess usage of power has a present or imminent impact on the ability of Service Provider to deliver redundant services to other customers within the STMS Data Centre (e.g. the Co-location Customer's distribution of equipment in its Customer Environment impacts power or cooling in the Customer Environment) then Service Provider may shut off that portion of the power supply services to the Co-location Customer as is required to alleviate the present or imminent impact on the integrity of Service Provider's business and systems. If reasonably possible in the circumstances, Service Provider will obtain Co-location Customer's specific instructions on which equipment should have its power supply shut off.

5.4 Data Centre Requirements Verification Process

The Province and Service Provider will follow the process (the "**Data Centre Requirements Verification Process**") described in this Section 5.4 to verify that the STMS Data Centres meet the Province's data centre infrastructure requirements described in Appendix G (*Data Centre Requirements*).

1. **Engineer**. The Data Centre Requirements Verification Process is based on periodic reviews carried out at or in respect of each STMS Data Centre (each, a "**Data Centre Requirements Verification**") by an independent consulting engineer (the "**Engineer**"). The Service Provider and the Province will agree on the identity of the Engineer for each Data Centre Requirements Verification. The Engineer will be retained by the Service Provider and the Service Provider will be responsible for the Engineer's fees. The Engineer will be required to enter into a non-disclosure agreement with the Service Provider and its STMS Data Centre Subcontractor to protect the confidentiality of the confidential and proprietary information of the Service Provider and its STMS Data

Centre Subcontractor made available to the Engineer in connection with the Data Centre Requirements Verification.

2. **Initial Data Centre Requirements Verification**. The initial Data Centre Requirements Verifications in respect of the STMS Calgary Data Centre and the STMS Interior Data Centre will each take place in accordance with the schedule set out in Schedule 10 (*Transformation Plan*) of the Agreement

   In connection with each initial Data Centre Requirements Verification, the Engineer will review the design and build of the STMS Data Centre in order to provide the Province with confirmation that the STMS Data Centre meets the requirements of the Province set out in Appendix G (*Data Centre Requirements*). The Engineer will provide the Province with a written report of the Data Centre Requirements Verification.

3. **Subsequent Data Centre Requirements Verifications**. In connection with each Data Centre Requirements Verification subsequent to the initial Data Centre Requirements Verification at an STMS Data Centre, the Engineer will review:

   (i) maintenance records and procedures for the power systems, fire systems and environmental systems at the STMS Data Centre in order to provide the Province with confirmation that the maintenance procedures for such systems at the STMS Data Centre meet or exceed the manufacturer's recommendations;

   (ii) any additional Customer Environment Area that has been built within the STMS Data Centre subsequent to the prior Data Centre Requirements Verification in order to provide the Province with confirmation that the expanded Customer Environment Area meets the Province's requirements as described in Appendix G (*Data Centre Requirements*).

   The Engineer will provide the Province with a written report of the Data Centre Requirements Verification.

4. **Timing**. The second Data Centre Requirements Verification in respect of each STMS Data Centre will take place approximately 4 years after the initial Data Centre Requirements Verification in respect of the STMS Calgary Data Centre. The third and subsequent Data Centre Requirements Verifications in respect of each STMS Data Centre will take place at four year intervals. The Parties will cooperate to allow the Data Centre Requirements Verifications in respect of the two STMS Data Centres to take place at approximately the same time.

5. **Co-operation**. The Service Provider will cooperate with the Engineer in connection with each Data Centre Requirements Verification in making available to the Engineer such information as the Engineer may require in order to provide to the Province the confirmations set out in this Section.

6. **Effort and Scheduling**. The Parties confirm their expectation that, in connection with each Data Centre Requirements Verification: (i) the Engineer will visit the STMS Data Centre that is the subject of the review; and (ii) the effort required of the Engineer for each Data Centre Requirements Verification should not exceed three weeks of effort.

Responsibility	Province	SP
Hire the Engineer to perform each Data Centre Requirements Verifications.		R
Approve the Engineer selected by the Service Provider to perform each Data Centre Requirements Verification.	A	
Service Provider to obtain, share with the Province and review the report produced by the Engineer in connection with each Data Centre Requirements Verification.		R
Service Provider to meet with the Province within one month following the receipt of the Engineer's report to discuss any issues.		R
With respect to any non-conformances identified by the Engineer's report on a Data Centre Requirements Verification, agree to remediation of such non-conformances during or within one month following the review meeting and the timeframe for such remediation measures to be implemented.		R
Implement the remediation measures agreed to by the Parties in respect of any non-conformances identified by the Engineer's report on a Data Centre Requirements Verification within the agreed to timeframe.		R

5.5 Data Centre Future Proofing

The STMS Data Centres Three Year Plans prepared by the Service Provider under Section 5.2 of this Part V of the Data Centre Services SOW will include a review of future information technology directions and an assessment of any requirements for technology changes at the STMS Data Centres. In connection with the STMS Data Centres Three Year Plans, Co-location Customers and the Province will provide the Service Provider with information concerning their likely future technology requirements including, if available, the timeframes within which and the likelihood that such future technology will be required.

The Province may conduct a benchmark comparison (the "**Data Centres Currency Benchmark**") of the technology currency of the technology located at the STMS Data Centres against industry standards for the technology currency of data centres, in accordance with the following:

(i) the benchmark comparison will not be performed more frequently than once every four Contract Years and will not be performed in the four year period after the Availability Date of the STMS Interior Data Centre;

(ii) the third party consultant performing the Data Centres Currency Benchmark will be selected by the Province, subject to the approval of the Service Provider;

(iii) the Province will be responsible for costs of the third party consultant retained to conduct the Data Centres Currency Benchmark;

(iv) the third party consultant retained to conduct the Data Centres Currency Benchmark shall be required to execute a non-disclosure agreement with Service Provider and its STMS Data Centre Subcontractor for access to any report produced during any Data Centre Requirements Verification; and

(v) the Service Provider will use commercially reasonable efforts to cooperate with the Province in connection with any such Data Centres Currency Benchmark, provided such cooperation will not interfere with the operation of the STMS Data Centres.

The Province will provide the Service Provider with a copy of any reports produced by the third party consultant conducting the Data Centres Currency Benchmark.

The Service Provider and the Province will review any requirements for technology changes at the STMS Data Centres as a result of future information technology directions and the future technology requirements of Co-location Customers, the Managed Services Customer and any Broader Public Sector entities that purchase Managed Services from the Service Provider. If a change in the technology of one of the STMS Data Centres is appropriate, the Service Provider will make reasonable efforts: (i) to implement such technology changes within the existing Customer Environment Area of the STMS Data Centres, so that the Co-location Customers, the Managed Services Customer or any Broader Public Sector entities that purchase Managed Services from the Service Provider are not required to relocate to another building phase of the STMS Data Centre or to another data centre to take advantage of the change in technology; and (ii) to spread the costs of required changes to common or shared infrastructure or facilities over the maximum number of customers.

If, at any time, a Co-location Customer has a requirement for agreed-to current technology in the STMS Data Centre that is not available in the STMS Data Centre at such time:

(i) the Co-location Customer will provide the Service Provider with as much notice of its requirements for the agreed to current technology at the STMS Data Centre as possible;

(ii) the Co-location Customer's notice of requirements for the agreed-to current technology at the STMS Data Centre will be deemed to be a Change Request under Section 7.4 (*Change Request*) of the Agreement and the Service Provider will provide the Co-location Customer with a Proposal for the implementation of such technology in the STMS Data Centre in accordance with the Change Order Process; and

(iii) if the Co-location Customer is required to relocate to another building phase of the STMS Data Centre in order to take advantage of the agreed to current technology, the Co-location Customer's Capacity Reservation in respect of the SMTS Data Centre will be forgiven to the extent of the capacity acquired by the Co-location Customer in the new building phase.

5.6 Province Capacity Reservation Reporting for Managed Services

5.6.1 Transformation Plan VA Reservation Calculation

Within three months following the end of the fifth Contract Year of the Agreement, a comparison will be made of actual VA usage for Managed Services for the Province in the sixtieth (60^{th}) month of the Agreement versus the VA usage projected for such services by the Service Provider in its Transformation planning assumptions for such month. More specifically,

(i) if the Adjusted Actual VA is greater than the Baseline VA, then the Service Provider will pay the Province one half the cost (calculated using the VA Unit Rate charged that month) of the difference between the Adjusted Actual VA and the Baseline VA; or

(ii) if the Baseline VA is greater than the Adjusted Actual VA, then the Province will pay the Service Provider one half the cost (calculated using the VA Unit Rate charged that month) of the difference between the Baseline VA and the Adjusted Actual VA.

As used in this Section 5.6, the following terms shall have the following meanings:

- **"Baseline VA"** shall mean 538,000 VA and is an amount equal to the sum of the Expected VA for all Baseline Units of all hardware devices (including Service Provider management tools and network devices) projected by the Service Provider in the Transformation planning assumptions to be required for the Managed Services for the Province in the sixtieth (60^{th}) month of the Agreement.

- **"Baseline Units"** shall mean, with respect to any hardware device (including Service Provider management tools and network devices), the number of units of such device projected by the Service Provider in the Transformation planning assumptions to be required for the Managed Services for the Province in the sixtieth (60^{th}) month of the Agreement.

- **"Expected VA"** shall mean, with respect to any hardware device (including Service Provider management tools and network devices), the number of VA's projected by the Service Provider to be consumed by such device. Expected VA's for Service Provider management tools and network devices are listed in Appendix E (*STMS Hosting Tools and Common Infrastructure Expected VA Consumption*) to this SOW.

- **"Change VA"** shall mean, with respect to any hardware device (including Service Provider management tools and network devices), an amount equal to (i) the difference between (a) the actual number of units of such device used for the Managed Services for the Province in the sixtieth (60^{th}) month of the Agreement, and (b) the Baseline Units of such device, times (ii) the Expected VA for such device.

- **"Total Change VA"** shall mean the sum of all Change VA.

- **"Actual VA"** shall mean, for any given month, the peak VA usage for the Managed Services for the Province.

- **"Adjusted Actual VA"** shall mean an amount equal to (i) the Actual VA usage from the sixtieth (60^{th}) month of the Agreement, less (ii) the Total Change VA for such month.

- **"VA Unit Price"** shall have the meaning assigned to such term in Schedule 23 (*Fees*) of the Agreement.

5.6.2 Annual VA Reservation Calculation

Within 3 months following the end of each Contract Year beginning with the third Contract Year of the Agreement, the Expected Tracked Total VA will be calculated. On the basis of such calculation,

(i) if the Expected Tracked Total VA for the month being measured is greater than the Actual VA for such month, then the Province will pay the Service Provider one half the cost (calculated using the VA Unit Rate charged that month) of the difference between such Expected Tracked Total VA and such Actual VA; or

(ii) if the Actual VA for the month being measured is greater than the Expected Tracked Total VA for such month, then the Service Provider will pay the Province one half the cost (calculated using the VA Unit Rate charged that month) of the difference between such Actual VA and such Expected Tracked Total VA.

As used in this Section 5.6, the term "**Expected Tracked Total VA**" shall mean an amount equal to the sum of the Expected VA for all hardware device units (including Service Provider management tools and network devices) actually used for the Managed Services for the Province.

VI. MEDIA DESTRUCTION AND EQUIPMENT DISPOSAL SERVICES

This Part VI of the Data Centre Services SOW is divided into two additional sections:

(i) Section 1 of this Part VI of the Data Centre Services SOW provides an introduction to the media destruction and equipment disposal services; and

(ii) Section 2 of this Part VI of the Data Centre Services SOW describes the services to be provided for media destruction and equipment disposal.

1. Introduction

This Part VI of the Data Centre Services SOW covers media destruction and equipment disposal. All asset disposal or media destruction will be in accordance with Province Policies, unless otherwise agreed in writing.

1.1 Sites

The media destruction and equipment disposal services will be provided for the following sites:

(i) Existing WTS Data Centres;
(ii) WTS Remote Sites; and
(iii) STMS Data Centres.

1.2 Effective Date and Term

This Part VI of the Data Centre Services SOW will be effective:

(i) with respect to each Existing WTS Data Centre on the Hand-Over Date and will continue in effect at each Existing WTS Data Centre other than the Province Designated Network Locations, until the WTS Data Centres Equipment End Date;

(ii) with respect to each of the Existing WTS Data Centres that is a Province Designated Network Location, until the later of: (1) the WTS Data Centres Equipment End Date for such data centre; and (2) the date that any routers or other communications equipment of the Service Provider installed at such data centre in accordance with Part IV (*Network Services*) of the Data Centre Services SOW are removed by the Service Provider;

(iii) with respect to each of the WTS Remote Sites on the Hand-Over Date and will continue in effect at each WTS Remote Site until the WTS Remote Sites Equipment End Date; and

(iv) with respect to each STMS Data Centre on the Availability Date of the STMS Data Centre and will continue through the expiration or termination of the Managed Services.

2. *Media Destruction and Asset Disposal Services*

This Part VI of the Data Centre Services SOW describes the scope and functions of the media destruction and equipment disposal process provided by the Service Provider at:

(i) the Existing S. 15 in Part II of Appendix D (Supported Province Locations); and
(ii) the STMS Data Centres.

Data Centre Services – WTS Sites	Province	Service Provider
Supply sufficient space within the secure computer room at the Existing WTS Data Centre location identified as S. 15 in Part II of Appendix D (*Supported Province Locations*) to store excess equipment ready for disposal and Lock Boxes to securely store Secure Storage Devices designated for disposal.	R	
Supply sufficient space to store excess equipment ready for disposal and Lock Boxes to securely store Secure Storage Devices within the Customer Environment for the Province at each STMS Data Centre.		R
For any Province-owned equipment or Service Provider-owned equipment that is managed by the Service Provider and has a faulty Secure Storage Device: (i) remove faulty Secure Storage Devices from the equipment; (ii) track the faulty Secure Storage Devices removed from the equipment; and (iii) deposit the faulty Secure Storage Devices into the available Lock Boxes.		R

Data Centre Services – WTS Sites	Province	Service Provider
For any Province-owned equipment or Service Provider-owned equipment that is managed by the Service Provider and is being disposed of: (i) remove Secure Storage Devices from the equipment; (ii) track the Secure Storage Devices removed from the equipment; and (iii) deposit the Secure Storage Devices into the available Lock Boxes.		R
Dispose of Service Provider provided equipment with Secure Storage Devices removed.		R
Make arrangements to deliver Lock Boxes with Secure Storage Devices and Province-owned equipment with Secure Storage Devices removed S. 15 S. 15		S. 15
Pay delivery fees for Lock Boxes with Secure Storage Devices and Province-owned equipment with Secure Storage Devices removed S. 15	R	
Pay AIR fees for media destruction and equipment disposal service.		R
Validate certification of media destruction provided by AIR based on tracking sheet of Secure Storage Devices provided by the Service Provider.		R
Notify Province of Province-owned equipment that has been disposed.		R

This Part VI of the Data Centre Services SOW describes the scope and functions of the media destruction and equipment disposal process provided by the Service Provider at:

(i) the Existing WTS Data Centre locations excluding the site identified as S. 15 Victoria, BC in Part II of Appendix D (Supported Province Locations); and
(ii) the WTS Remote Sites.

Data Centre Services – WTS Sites	Province	Service Provider
Supply sufficient space to store excess equipment ready for disposal and Lock Boxes to securely store Secure Storage Devices within a secure room of the Service Provider's office location in Victoria, BC.		R
For any Province-owned equipment or Service Provider-owned equipment that is managed by the Service Provider and has a faulty Secure Storage Device: (i) remove faulty Secure Storage Device from the equipment; (ii) track the faulty Secure Storage Devices removed from the equipment; and (iii) Securely Ship the faulty Secure Storage Devices to the Service Provider's office location in Victoria, BC.		R
For any Province-owned equipment or Service Provider-owned equipment that is managed by the Service Provider and is being disposed of: (i) remove Secure Storage Devices from the equipment; (ii) track the Secure Storage Devices removed from the equipment; and (iii) Securely Ship the faulty Secure Storage Devices to the Service Provider's office location in Victoria, BC.		R
Make arrangements to deliver Province-owned equipment with Secure Storage Devices removed to AIR through either of two approved methods: S. 15		R
Dispose of Service Provider provided equipment with Secure Storage Devices removed.		R
Validate Secure Storage Device(s) shipments received from other sites against tracking and deposit Secure Storage Device(s) into the available Lock Boxes located at the Service Provider's office location in Victoria, BC.		R
Make arrangements to deliver Lock Boxes containing Secure Storage Devices to AIR through either of two approved methods: S. 15		R
Pay delivery fees for Lock Boxes with Secure Storage Devices and Province-owned equipment with Secure Storage Devices removed that were shipped to AIR.	R	
Pay AIR fees for media destruction and equipment disposal service.		R

Data Centre Services – WTS Sites	Province	Service Provider
Validate certification of media destruction provided by AIR based on tracking sheet of Secure Storage Devices provided by the Service Provider.		R
Notify Province of Province-owned equipment that has been disposed.		R

Appendix A – Defined Terms / Definitions

Definable Term	Definition
7 x 24	*24 hours per day, 7 days per week, 52 weeks per year*
Access Control List (ACL)	*A list used to control access to information or resources. The list contains the user identifiers and/or group identifiers that are allowed access to the information or resources.*
Actual VA	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Adjusted Actual VA	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
AIR	*Asset Investment Recovery, a branch of the Province of British Columbia's Procurement and Supply Services*
Applicable Laws	*As defined in the Agreement*
Availability Date	*Means, for each specific STMS Data Centre, as applicable, the date set out in Section 3.2 of the Transformation Statement Of Work forming part of Schedule 9 – Transformation Schedule.*
Baseline VA	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Baseline Units	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Broader Public Sector ("BPS")	*Has the meaning attached to such term in the Agreement*
Buyers	*Members of the Broader Public Sector who acquire services from the Service Provider under the JSRFP pursuant to separate services agreement with the Service Provider.*
Cage	*Physically secure environment in the raised floor area of a data centre that includes cage wall material and entrances that are secured with biometric access controls. See details in Service Catalogue.*
Capacity Reservation	*Means, with respect to any Co-location Customer or any Managed Services Customer or any Broader Public Sector that purchase Managed Services from the Service Provider, that portion of the Province VA Commitment that the Province has allocated to that Co-location Customer or Managed Services Customer or Broader Public Sector entity that purchased Managed Services from the Service Provider.*
Change Order Process	*As defined in the Agreement*
Change VA	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Co-location	*Services that house an organization's servers and applications. The co-location provider is typically responsible for supplying power, lights, cooling and the physical security of the site.*
Co-location Customers	*Has the meaning attached thereto in Section 1.3 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Common Data Centre Features	*Has the meaning attached thereto in Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Core STMS Data Centre Services	*Has the meaning attached thereto in Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Customer Environment	*Has the meaning attached thereto in Section 1.3 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Customer Environment Area	*The area within each STMS Data Centre available for the location of Customer Environments (often referred to as the "raised floor" area of the data centre).*
Data Centre	*A facility dedicated to providing power, cooling, fire control and physical security to computer systems located within it.*

Definable Term	Definition
Data Centre Services	*As defined in the Agreement*
Data Centre Access Agreement	*A document to be signed by a Visitor at an STMS Data Centre that acknowledges the Visitor's acceptance of the rules and guidelines for their access to the facility and conduct while physically present at the data centre.*
DCPO or Data Centre Protection Officer	*Has the meaning attached thereto in Section 2.1 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Data Centre Currency Benchmark	*A benchmark comparison of the technology currency of the technology located at the STMS Data Centres against current industry standards as further described in Section 5.5 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Data Centre Requirements Verification	*Has the meaning attached thereto in Section 5.4 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Data Centre Requirements Verification Process	*Has the meaning attached thereto in Section 5.4 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Engineer	*Has the meaning attached thereto in Section 5.4 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Environment Controller	*Has the meaning attached thereto in Section 1.3 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Environment Controller Provided Enclosure	*A rack or cabinet that is provided by an Environment Controller for installation in their Cage(s).*
Environment Controller Provided Equipment	*Computing hardware that is owned or supplied by a Environment Controller that is physically located in a Customer Environment.*
Existing WTS Data Centres	*Has the meaning attached thereto in section 1.3 of Part I of the Data Centre Services SOW*
Existing WTS Data Centres Services	*Has the meaning attached thereto in Part II (Existing WTS Data Centres Services) of the Data Centre Services SOW*
Expected VA	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Hands and Eyes	*A service that makes on-site operations staff available within an STMS Data Centre to work under the Environment Controller's direction to perform specific functions and assist in urgent situations (see Service Catalogue for more information and examples).*
HVAC	*An acronym that stands for "heating, ventilating, and air conditioning".*
Information Technology ("IT")	*The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.*
KW	*Kilo Watt*
Local Area Network (LAN)	*A computer network covering a small physical location, or a small group of buildings, such as a school, or an airport*
Lock Boxes	*Extra Large lock boxes measuring approximately 20.5 inches long by 28 inches wide and 19 inches high that are provided at no charge by the Province (through AIR).*
MAC	*Media Access Control – the MAC address is a quasi-unique identifier assigned to most network adapters or network interface cards by the manufacturer for identification.*
Managed Equipment	*The servers, storage, and backup equipment for which the Service Provider is providing Services under the Service Management*

Definable Term	Definition
	Services SOW, the Transformation SOW, the Business Continuity and Disaster Recovery Services SOW, the Security Services SOW, the Managed Mainframe Services SOW, the eight (8) Midrange Services SOWs (Server Management Services SOW, Shared File and Print Services SOW, Web Hosting Services SOW, Virtual Hosting Services SOW, Onsite Support Services SOW, Citrix Based Computing Services SOW, Shared Database Services SOW, and the Application Enabling Services SOW), and the Storage and Backup Services SOW.
Management Network	*The management network implemented by the Service Provider pursuant to the Network LAN/WAN Transformation Project described in Section 6 of the Transformation SOW.*
Managed Services	*As defined in the Agreement.*
Managed Services Customer	*Has the meaning attached thereto in Section 1.3 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
N+1 Redundancy	*"N+1 redundancy" means a system design where one additional component of spare capacity (+1) is added to the total number of primary components required by that system (N) in order to reduce the exposure to faults in any single component.*
NFPA-75	*"Standard for the Protection of Information Technology Equipment" published by the National Fire Protection Association, as such standard is in effect at the Hand-Over Date.*
Optional STMS Data Centre Services	*Has the meaning attached thereto in Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
PDUs	*Power Distribution Units*
Periodic Capacity Review Meetings	*Has the meaning attached thereto in Section 5.2 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
Physical Space	*The portion(s) of an STMS Data Centre made available to the Environment Controller for the placement of Environment Controller Provided Equipment.*
Province Designated Network Locations	*The Existing WTS Data Centres located at* S. 15 S. 15
Province Network	*SPAN/BC*
Province VA Commitment	*Has the meaning given to it in Schedule 23 (Fees).*
PSTN	*Public Switched Telephone Network*
RASIC	*A Model used to help define Responsibilities. RASIC stands for Responsible, Accountable, Supporting, Consulted and Informed.*
Q9 Biometric Access Control System	*The security control system used to monitor and control access within the STMS Data Centres.*
Q9 Control Panel	*A secure web site that provides customers with access to their account information and visibility into critical aspects of their environment.*
Q9 Customer Guide	*A document available through the Q9 Control Panel outlining certain information, rules, guidelines and procedures with respect to the STMS Data Centres.*
Q9-Cabinet	*Locked cabinet with front and back doors and space for 42U of equipment. See details in Service Catalogue.*
Q9 Power Monitoring and Reporting Services	*A service that provides Environment Controllers with reports that summarize their current and aggregate peak power demand in a given STMS Data Centre on both an aggregate and detailed circuit level basis.*
Secure Storage Device	*Storage Devices (as defined in this table) that have been used to store Province data.*
Securely Ship	*Shipments made through either of the following methods:*

Definable Term	Definition
	S. 15
Service Locations	*As defined in the Agreement*
Service Provider Network Equipment	*As defined in Section 2 of Part IV of the Data Centre Services SOW*
Service Provider Network Equipment End Date	*As defined in Section 1.2 of Part IV of the Data Centre Services SOW*
Service Provider Support Locations	*Service Locations of the Service Provider or its Subcontractors.*
Services	*As defined in the Agreement.*
SF	*Square Foot*
STMS Calgary Data Centre	*The STMS Data Centre located in Calgary, Alberta.*
STMS Data Centre Total Contracted Capacity	*With respect to any STMS Data Centre and at any time, the total committed power capacity of all customers in such STMS Data Centre.*
STMS Data Centres	*Has the meaning attached thereto in Section 1.3 of Part I (Introduction) of the Data Centre Services Statement of Work.*
STMS Data Centre Services	*Has the meaning attached thereto in Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
STMS Data Centres Three Year Plan	*Has the meaning set out in Section 5.2 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work.*
STMS Interior Data Centre	*The STMS Data Centre to be located in the interior of the Province of British Columbia.*
Storage Device	*The following devices: hard drives (IDE, SCSI, ATA, portable, micro drives, laptops), removable/transportable digital memory media, digital memory card, multi-media memory cards, USB memory sticks/drives or thumb drives, compact flash drives, smart cards, flash cards, memory cards, subscriber identity module cards, ZIP disk, floppy disks, and magnetic tapes.*
Third Party Gateway	*The security mechanisms implemented by the Province to control third party access to SPAN/BC.*
Total Change VA	*Has the meaning attached thereto in Section 5.6 of Part V (STMS Data Centre Services) of the Data Centre Services Statement of Work*
Uninterrupted Power Supply ("UPS")	*The components of the data centre power system that condition raw utility power and provide continuous power during the switch-over from power provided by the public utility to power provided by the on-site generators.*
VESDA® (Very Early Smoke Detection Apparatus)	*Very Early Smoke Detection Apparatus, a particular brand of aspirating smoke detector.*
Virtual Local Area Network (VLAN)	*A group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location.*
Visitor	*Any individual employee, agent, contractor or representative of an Environment Controller and who is requesting access to an STMS Data Centre.*
Volt-Amp (VA)	*A volt-amp (VA) is a unit of aggregate power demand. VAs are calculated by summing the current drawn (in amps) on each phase of each circuit supplying power to the Environment Controller Provided Equipment and then multiplying the resulting sum by 120 volts.*

Definable Term	Definition
WTS Data Centres Equipment	*The servers, storage, and backup equipment that is located at the Existing WTS Data Centres for which the Service Provider is providing Services under the Service Management Services SOW, the Transformation SOW, the Business Continuity and Disaster Recovery Services SOW, the Security Services SOW, the Managed Mainframe Services SOW, the eight (8) Midrange Services SOWs (Server Management Services SOW, Shared File and Print Services SOW, Web Hosting Services SOW, Virtual Hosting Services SOW, Onsite Support Services SOW, Citrix Based Computing Services SOW, Shared Database Services SOW, and the Application Enabling Services SOW), and the Storage and Backup Services SOW.*
WTS Data Centres Equipment End Date	*Has the meaning attached thereto in section 1.2 of Part II of the Data Centre Services SOW.*
WTS Remote Sites	*Has the meaning attached thereto in section 1.2 of Part I of the Data Centre Services SOW.*
WTS Remote Sites Equipment	*The servers, storage, and backup equipment that is located at the WTS Remote Sites for which the Service Provider is providing Services under the Service Management Services SOW, the Transformation SOW, the Business Continuity and Disaster Recovery Services SOW, the Security Services SOW, the Managed Mainframe Services SOW, the eight (8) Midrange Services SOWs (Server Management Services SOW, Shared File and Print Services SOW, Web Hosting Services SOW, Virtual Hosting Services SOW, Onsite Support Services SOW, Citrix Based Computing Services SOW, Shared Database Services SOW, and the Application Enabling Services SOW), and the Storage and Backup Services SOW.*
WTS Remote Sites Equipment End Date	*Has the meaning attached thereto in section 1.2 of Part III of the Data Centre Services SOW.*
WTS Remote Sites Services	*Has the meaning attached thereto in Part III (WTS Remote Sites Services) of the Data Centre Services SOW.*
WTS	*The information and technology division of the Ministry of Labour and Citizens' Services of the Province of British Columbia known as Workplace Technology Services, and any successor thereto.*

Appendix B – Reports

This appendix includes information related to reports that apply to each Part of the Data Centre Services SOW. This appendix is divided into parts as they relate to each Part of the Data Centre Services SOW.

I. NOT APPLICABLE

II. EXISTING WTS DATA CENTRES

1 Reports by Province

1.1 Current Data Centre Load Charts

This is a weekly WTS report produced by the Province to track the power and cooling loads in the Existing WTS Data Centres.

Frequency: Weekly
Distribution: Via email

Format: Excel spreadsheet
Spreadsheet Tabs (worksheets):

- Capacity Summary
- Capacity Status Data Centres
- Monthly Report
- Weekly Report
- Capacity Summary RNC's
- RNC's Raw Data
- Floor Space
- Server View
- Raw Data
- Input Field

S. 15

Sample Report: 
D:\Documents and Settings\qzs7

2 Reports by Service Provider

2.1 Monthly Router Performance Report

This is a monthly report produced by the Service Provider to show numerous charts of performance metrics for a given router under its control.

Frequency: Monthly
Distribution: Via email
Format: PDF
Report details: The following performance charts are included:

- Total Bytes (bytes/sec)
- Total Packets (packets/sec)
- Total Queue Drop In & Out (packets/sec)
- Total Queue Discards (packets/sec)
- Total Errors (errors/sec)
- Latency (msec)
- Availability %
- Free Memory (bytes)
- CPU Utilization %
- Memory Utilization %
- Slow Packets Out (packets/sec)

III. NOT APPLICABLE

IV. NOT APPLICABLE

V. STMS DATA CENTRE SERVICES

1 Reports by Service Provider

1.1 Power Reports

Power utilization reports detailing capacity and peak measurements available in both daily and monthly views.
Frequency: Online – on request
Format: HTML (tabular format) and also available for download in CSV format

1.2 Enclosure Power Detail Reports

Power reporting of an enclosure providing point-in-time snapshots of current utilization on a per-circuit basis.
Frequency: Online – on request
Format: HTML (tabular format)

1.3 Data Centre Ticketing System

Progress reporting of Environment Controller's tickets (active, closed, all tickets, or custom search).
Frequency: Online – on request
Format: HTML (tabular format)

1.4 Bandwidth Reports

Environment Controller daily, weekly, monthly, and past 12 months Internet bandwidth utilization reports displaying a graph of the daily Internet bandwidth usage. Daily graphs are provided in 5-minute averages. This report is only available if Environment Controller is using one of the bandwidth optional services.
Frequency: Online – on request
Format: HTML (tabular format)

VI. NOT APPLICABLE

Appendix C – STMS Hosting Tools and Common Infrastructure Expected VA Consumption

	Device	Function	Expected VA
Tool Servers			
	Backup Media Servers		450
	Citrix Admin Server		387
	Opsware server		298
	CA DSM server		298
	Network TNMIP servers		510
	Network eHealth reporting server		298
	VMware Consolidated B/U		359
	VMWare VC servers		359
	NetQoS appliance (or Introspect)		298
	EAS Exch Server		298
	EAS File Server		298
	EAS AD DC		298
	AIX HMCA		450
	Duper		510
	Client Facing Web Portal		220
	SSMSV2_ECC/Repository Servers		298
	SSMSV2_Store Servers		220
	SSMSV2_Agent Servers		220
	SSMSV2_WLA Archiver		220
	SSMSV2_Terminal Server		298
	SSMSV2_Remote Agent Servers		220
	IPS Server		220
	Unix Jump server		281
	SSMS-IPS; EMC Backup Advisor		450

	Device	Function	Expected VA
Network			
	Cisco 6509	LAN Switch - large	6000
	HP 3500yl-48	LAN Switch - medium	185
	Load Balancers	Included in 6509	
	Cisco Router	Router - medium	150
Security			

S. 15

Mainframe	Model	Detail	Expected kVA
Processor & Consoles	IBM 2096-S03	617 MIPS	5.9
DASD	EMC DMX4-950	3525 GB	4.3
Switch	Cisco 9134	2 switches	0.4
Tape	STK VSM 16 TB	16TB	3.8
Tape	STK SL8500+1 SEM+8 Drives	145TB	3.9
Swing Hardware (Nov. 2010 to June, 2011)			
Tape	IBM 3490 Tape drives	24 drives	9.6
Tape	IBM 3494 library, VTS and 3590 drives	6 drives, 16GB VTS	8.0
Disk	HDS 9900V	3525GB	34

Appendix D – Supported Province Locations

This appendix includes information related to the supported Province locations that apply to each Part of the Data Centre Services SOW. This appendix is divided into parts as they relate to each Part of the Data Centre Services SOW.

I. NOT APPLICABLE

II. EXISTING WTS DATA CENTRES

WTS Data Center Location	Visitor Work Space	Size (SF)	Capacity (KW)	Load (KW)	Available (KW)	Expansion Plans	Expansion (KW)
S. 15							S. 15

Table D.1 Existing WTS Data Centres

The information in Table D.1 with respect to Size (SF), Capacity (KW), Load (KW), Availability (KW), Expansion Plans and Expansion (KW) is as of December 19, 2008.

III. WTS REMOTE SITES

WTS Remote Sites	Building Type	Room Number
S. 15		

WTS Remote Sites	Building Type	Room Number
S. 15		

Table D.2 WTS Remote Sites

The information in Table D.2 is as of February 26, 2009.

IV. NOT APPLICABLE

V. NOT APPLICABLE

VI. NOT APPLICABLE

Appendix E – Service Provider Service Locations

This appendix includes information related to the Service Provider service locations that apply to each Part of the Data Centre Services SOW. This appendix is divided into parts as they relate to each Part of the Data Centre Services SOW.

I. NOT APPLICABLE

II. NOT APPLICABLE

III. NOT APPLICABLE

IV. NOT APPLICABLE

V. STMS DATA CENTRE LOCATION

There are two STMS Data Centre sites:

(i) STMS Calgary Data Centre – which is a new data centre that is under construction in Calgary, Alberta; and

(ii) STMS Interior Data Centre – which is a new data centre construction project in the interior of the Province of British Columbia that will start after the Effective Date.

Province will be required to sign a non disclosure agreement before receiving information concerning the location of the sites. A separate non disclosure agreement will be required for each site.

The VA capacity of the STMS Data Centres is defined in the following table:

STMS Data Centre	Minimum Initial Build VA Capacity	Minimum Potential VA Capacity
STMS Interior Data Centre	1,800,000	3,600,000
STMS Calgary Data Centre	1,800,000	7,200,000

VI. NOT APPLICABLE

Appendix F – WTS Data Centre Infrastructure Capacity Request/Approval Process

WorkPlace Technology Services
Data Centre Infrastructure Capacity
Request/Approval Process
Effective November 20, 2006

Introduction
This document describes the request and approval process that must be completed prior to the installation of hardware in any of the WTS Data Centres. This process replaces all other hardware request/approval procedures as of Nov 20, 2006 and shall remain in effect until the Data Centre project team institutes a permanent request/approval procedure.

Audience
This document is intended for the individuals who are routinely involved in hardware procurement and installation in the WTS data centres, specifically the various Hosting Branch groups – Windows, AES, Storage and Network. It is also intended for the WTS data centre facility management team and Hosting branch executive. Its purpose is to clearly outline the process and responsibilities of these groups when new or additional hardware needs to be installed in a Data Centre.

Process
This process is initiated upon receipt of a firm [1]Client request for server, storage or network hardware needing to be placed in a WTS Data centre. Once received, the request needs to be translated into specific hardware specifications so that the proper approvals can be given once adequate space, cooling, power and network connectivity has been confirmed. Only then can procurement and installation of the hardware proceed. The process is outlined in the following diagram:

[1] A request is considered to be 'firm' when Clients have already agreed to pay the costs involved, or when it has been determined that it is very likely that the Clients will agree to the costs involved.

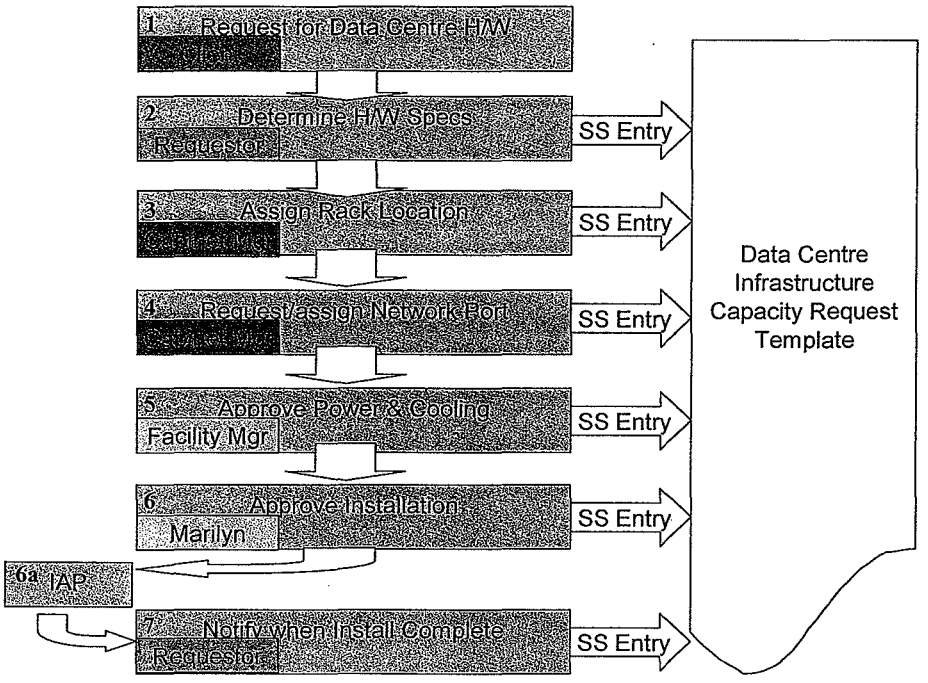


Figure 1: Request/Approval Process

Step 1 – Request for Hardware Received
In this step, a request for hardware that needs to be installed in one of the WTS Data Centres is received. This request can be either from a Client organization, or from an internal customer. If a CBA receives the request, they must forward it to the appropriate hosting group for processing. If the request is received by a hosting group, they should work with the CBA to ensure the next steps are initiated. In the case of Windows Hosting requests, the request must come from a client with approval authority for the purchase and be accompanied by a billable charge code in order to be considered 'firm'.

Step 2 – Determine Hardware Specifications
In this step, the appropriate hosting group assigns a "requestor", who must determine the specifications of the requested hardware with respect to power consumption, heat output and space and network connectivity requirements. The requestor enters this information in a new spreadsheet using the Data Centre Infrastructure Capacity Request Template located at http://gww.mser.gov.bc.ca/WTS/approvalprocess/process.htm#chgmgmt, and emails it to the appropriate cabinet space manager (the Windows Hosting, Open Systems, Network and Application Enabling Groups each have a separate cabinet space manager).

Step 3 – Assign Cabinet Location
Upon receipt of the request, the cabinet space manager assesses the available cabinet space and reserves a location for the hardware to be installed. This information is entered into the request spreadsheet. If network connectivity is already present in the cabinet, the cabinet space manager can enter this information in the spreadsheet and skip step 4.

Step 4 – Request Network Port Assignment (if required)
If this step is required, the process is put on hold until the install of network switches is approved and completed. As this may take a significant amount of time, the cabinet space manager should

provide feedback to the requestor about the delay in overall approvals. This information should in turn be relayed back to the Client via standard channels.

As required, the cabinet space manager requests additional network ports from the Network Operations Group (currently via email, new process tbd). If the request results in a requirement for additional network hardware to be installed in the Data Centre, Network Operations shall submit a hardware request using this process, starting at Step 2. Once the network port has been assigned, the cabinet space manager enters the cabinet location information in the request spreadsheet and emails it to the facilities manager.

Step 5 – Approve Power & Cooling

Upon receipt, the facility manager reviews the hardware specifications in the request spreadsheet and evaluates the new requirement against the current facility capacity. If the request falls within specified power and cooling thresholds, approval to proceed can be granted, and the request is entered in the master DCC tracking spreadsheet. The facility manager enters his/her approval in the appropriate column in the DCC tracking spreadsheet and notifies the installation approver, cc'ing the requestor, cabinet space manager, & CBA.

If the request falls outside of the specified power and cooling thresholds, the facility manager must notify the CBA, requestor, cabinet space manager and installation approver so that contingencies may be examined and options presented to the requesting Client.

Once approval is given to install hardware, the facility manager must also add the power and cooling requirements for the particular request to the "reserved" total on the facility's power and cooling capacity status tool.

Step 6 – Approve Installation

Once notified by the facility manager, the Installation Approver can be assured that all requirements have been identified and confirmed as being within the specified cooling, power, space and network connectivity thresholds, and can approve the installation. The Installation Approver shall indicate their approval by a "reply all" to the facility manager's email, instructing the server technician to proceed with the hardware purchase approval process.

Step 6a – IAP

If the request is not funded by a Client, it is at this point that the server technician provides the costing information to the CBA for procurement approval via the WTS Investment Approval Process (IAP). Once approval is obtained, the CBA will notify the requestor, who can then proceed with the hardware procurement and installation.

Step 7 – Notify When Installation Complete

Once approval has been granted, the requestor shall proceed with procurement and installation activities. When these activities are complete and the hardware is operational, the requestor shall notify the facility manager of this fact so that the power and cooling requirements can be removed from the "reserved" total on the facility's power and cooling capacity status tool. This signals the end of the Data Centre Infrastructure Capacity Request and Approval process.

Spreadsheet Format & Instructions

It is imperative that the Data Centre Infrastructure Capacity Request Template is filled out in a consistent manner, to ensure accurate reporting of power, space, cooling and network requirements. What follows is a description of the data required in each of the column headings in the spreadsheet, and the format in which it should be input.

Column Heading	Data and Format
Request #	This column is a sequential numbering of requests – add one to the previous line item
Request Date	Input the date the request is entered in the spreadsheet by the server technician (not when it was received from the Client)
Name of Installer	The name of the person who will physically install the device in the Data Centre - this will be the requestor in most cases.
Requestor's Group	The requestor's group - E.G. – WINHOST, OSG, AES, etc..
Client Org.	The client organization requesting the hardware. If WTS, indicate the business group in brackets e.g. (CAS), (BTI), (Ntwk), etc
Planned Date of Change	Indicate when the actual physical activity in the Data Centre is to take place – if unsure of exact date, indicate the month.
Hardware Type	Indicate whether the hardware is a server, switch, storage device, etc. Generic hardware categories such as these are to be used, not brand or model specifics.
Hardware Network Identification	Indicate the network identification name, preferably in a Fully Qualified Domain Name format – e.g. "spring.gov.bc.ca". If not known at the time the request is made, indicate "tbd".
Type of activity	Indicate whether the activity is an "install", "removal", or "swap" by picking from the drop-down list. A swap is defined as a direct replacement of identical hardware using the same FQDN, completed in one day. If the activity is a change from one type of hardware to another, or if there is a delay of more than 24 hrs between the start and end of the "swap", use two separate lines to indicate a "removal" and a separate "install" instead. Similarly, transfers from one Data Centre to another should be indicated by a "removal" at one site, and an "install" at the other.
Data Centre Site	Indicate the street address of the Data Centre where the hardware is to be installed by picking from the drop-down list.
Alternate Site acceptable? (Y/N)	Indicate whether the hardware can be placed in a different site than the one indicated in the "Data Centre Site" column. WTS reserves the right to determine where hardware is installed based on network and facility considerations. Requests for installations at some lower capacity Data Centre sites may require further justification and will be subject to the WTS Data Centre Site prioritization process.
# Cabinet Units	Data Centre standard cabinets are 19" wide x 36" deep, with vertical space divided into standard 1.75" high units. Hardware space requirements should be expressed in the number of standard units required.
Power Connector Type	Indicate the type of plug utilized by the hardware. There are many types of plug, and it is best to indicate the NEMA type if known. More information on the various NEMA plug types can be obtained from the facility manager.
Number of Connections required	Indicate the actual number of power connections that will be use by the hardware – do not indicate the theoretical maximum as specified by the manufacturer unless they will all be used.
Voltage and Amperage	Operating voltage and amperage as per manufactures specification. List typical and maximum and specify 3 phase if required.
Power	Indicate the typical and maximum power consumption of the device as

Column Heading	Data and Format
Consumption	measured in Watts.
VA rating	Rating in Volt Amps typical and maximum.
Max Thermal Output	Indicate the maximum thermal output of the device in BTU/hr (British Thermal Units per Hour).
Operating Temperature	Indicate the typical operating temperature in degrees Celsius.
Network Connections - # required	Indicate the number of network connections required for general network connectivity – do not include console connections.
Network Connections – Speed	Indicate whether a 100Mbps or a Gigabit connection is required.
Proposed IP Range	Where known, indicate the IP range (or subnet) the device will reside in. Use the form S. 15
Storage Network - # connections required	Indicate the number of fibre network connections required for SAN connectivity.
Target Storage Device(s)	Indicate by name which storage unit the new device will be connected to. Note that new storage devices require a separate row in the request spreadsheet.
Assigned Room	This column will be filled in by the cabinet space manager, and will indicate the room where the device will be installed.
Assigned Cabinet	This column will be filled in by the cabinet space manager, and will indicate the number of the cabinet where the device will be installed.
Pwr/AC & Space approval	This column will be filled in by the facility manager ("Yes" or "No") and indicates that sufficient power, cooling and space capacity exists in the requested Data Centre to accommodate the request.
Install Approval	This column will be filled in by the facility manager upon receipt of installation approval ("Yes" or "No") and indicates that the request has been authorized to proceed to procurement and installation.
Complete	This column will be filled in by the facility manager upon receipt of installation notification for the device.

Contact Information

	Primary Contact	Secondary Contact
Facility		
Windows Hosting		
Open System Group		
Storage and Backup		
Network		
Approvals		

Data Centre
frastructure Cap

Data Centre Infrastructure Capacity Request Template:

Appendix G – Data Centre Requirements

The STMS data centres will meet certain minimum requirements as described in the table below.

Item	Requirement
Delivery paths	The power system will provide at least two delivery paths within the facility
Redundancy	See statements in specific power and cooling sections below.
Concurrently maintainable	Critical power and cooling systems will be designed such that routine maintenance does not require a power or cooling interruption to customer critical loads.
Usable for critical load	The Province will be able to use 100% of their currently reserved power demand.
Uninterruptible cooling	A portion of the cooling systems will be powered by UPS systems.
Floor loading lbs/SF	At least 150lbs per square foot can be accommodated.
Single points of failure	Critical power and cooling systems will be designed to avoid single points of failure.
Site availability	Each data centre will be engineered to be available at least 99.98% of the time.
Transient voltage suppression system	Power systems will include multiple transient voltage suppression systems.
Telecommunications entrances	Each data centre will have at least 2 diverse building entrances for telecommunications cabling.
Power generators	Generator power system will be at least N+1.
Generator battery configuration	Generator battery system will be at least 2N.
Generator fuel storage	Each data centre will have sufficient onsite fuel storage to support 48 hours of generator power at design load.
Load bank	Each data centre will have a load bank onsite that is accessible to power generators through switch reconfiguration.
UPS redundancy	UPS systems will be sized to the data centre load and provide at least N+1 redundancy.
Critical power distribution	Within the facility, critical power will be distributed via dual paths to match the load.
Cooling plant	The cooling plant will be at least N+1.
Water storage / domestic water supply	Critical cooling will not be dependent on municipal water supply availability.
Piping distribution	Critical cooling will not be dependent upon the availability of a single piping section or valve.
Environmental air conditioners	Environmental systems will be engineered to be at least N+1 redundant per zone.
Building management system	A building management system will be engineered, including centralized monitoring.
Fire protection above raised floor	Each data centre will include a pre-action, dry-pipe sprinkler system.
Fire protection below raised floor	Fire protection below the raised floor will, at a minimum, meet code requirements.
Fire protection in non-critical spaces	Fire detection and suppression systems deployed in other non-critical areas in each data centre will, at a minimum, meet code requirements.

Appendix H – Energy and Environmental Efficiency

This appendix outlines topics involving energy and environmental efficiencies in the SMTS Data Centres.

General Benefits of Moving to New STMS Data Centres

As a general principle, larger facilities are more efficient to operate. The STMS Data Centres will achieve efficiencies through consolidating data centre requirements from several small, separate facilities into two larger data centres that will support not only the requirements of the Province and participating Broader Public Sector organizations, but also the commercial market as well.

As a general principle, new facilities also provide an opportunity to use newer power and cooling technologies that are usually more energy efficient and environmentally responsible compared to the technology deployed in existing, older facilities.

STMS Pricing Model Encourages Efficient Use of Power and Cooling Resources

The pricing model used for the STMS Data Centres is based on power demand (versus square feet). This pricing method allows each customer to receive its share of all of the data centre's key resources: space, power and cooling. It also provides a direct economic incentive to the customers to make efficient use of the power and cooling resources provided in the STMS Data Centres.

A pricing model based on a cost per square foot of data centre space provides an inherent incentive to customers to concentrate their equipment in a smaller than required footprint on the Data Centre floor. This results in some areas in the Data Centre with high-density cooling requirements and some areas with low (or no) cooling requirements. This type of uneven distribution can result in an inefficient and wasteful use of cooling system capacity.

The power demand pricing model provides no economic incentive to make inefficient use of cooling system capacity. Further, Province and Buyers (and other commercial customers) are all required to distribute their equipment as evenly as possible throughout their physical environment so as to make efficient use of each STMS Data Centre's cooling resources.

Power Monitoring and Reporting Ensures Energy Awareness

Fundamental to any approach to improving or maintaining energy efficiency is understanding how much power is being used (and when and where it is being used). Each Customer Environment will be provisioned with the Q9 Power Monitoring and Reporting Services. This service will provide customers with reports that summarize their current and aggregate peak power demand in a given STMS Data Centre on both an aggregate and detailed circuit level basis. Each customer, at its option and expense, will be able to use this service to:

- Establish benchmarks for energy efficiency and measure their progress towards reduced energy consumption in comparison to these benchmarks
- Identify and correct uneven power (cooling) density distribution (to ensure efficient use of cooling resources)

Contracting Based on Total Province Power Demand Ensures Efficient Use of Capacity

As a general principle, data centres are most efficient when operated at or near their capacity. It is inefficient to have some customers reserve capacity that they aren't using. The Province is contracting on behalf of itself and Broader Public Sector organizations (as described in Part V (*Data Centre Services*) of the Data Centre Services SOW) so that capacity can be redistributed amongst the Province parties in order to better match variations in requirements from time to time. Overall, this contracting approach allows the data centre capacity to be used more efficiently.

Possible Additional Technologies and Operating Methods to Improve Energy Efficiency and Reduce Environmental Impact

In designing and building the new SMTS Data Centres additional methods and technologies for improving energy efficiency and reducing the environmental impact of the STMS Data Centres have been and will continue to be considered. Evaluation of the suitability of these different methods and technologies will be balanced by three factors:

1. Is there an impact to the operational reliability in the Data Centre?
   The top priority in all STMS Data Centres is to continue to offer reliability and performance to the Province and Buyers in accordance with the terms and conditions of the Master Services Agreement and the BPS Services Agreement, as applicable. Given the critical nature of the IT operations that will be deployed within the STMS Data Centres, the Province and Buyers (and other commercial customers), typically have no tolerance for the implementation of a technology or operating method that would reduce the levels of reliability in the key data centre systems (such as power, cooling, security and fire systems).

2. Is there a positive business case?
   Service Provider will consider whether the initial capital investment in new technologies and operating methods pays back within a reasonable time period through savings in operational expenses.

3. Is there an impact to the design/build timeline?
   The Province and Buyers have urgent requirements for the availability of initial capacity in each STMS Data Centre. Service Provider will consider the possible impact to the build timeline of implementing new technologies and operating methods designed to achieve improvements in energy efficiency and environmental impacts.

The standard build design used as basis for the STMS Data Centres includes energy efficient power and cooling systems. In general, there is a strong business case supporting the investment in most of these systems and the projected build timelines incorporate their use.

STMS Hosting Services

SECURITY SERVICES – STATEMENT OF WORK

Table of Contents

1. GENERAL INFORMATION

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in Appendix A of this SOW, and as defined in the other SOWs and the Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meaning given to them.

1.2 Responsibility Charts

This SOW contains charts that describe the responsibilities of the Province and the Service Provider in respect of the Security Services, as indicated in the charts by an "R", to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.3 Security Services

Security Services provide the implementation of security controls and delivery of security services in compliance with the Province security requirements as defined in this document. The purpose of this SOW is to describe the scope and functions of the Security Services to be performed by Service Provider for the Province under the terms of the Agreement. The services described in this SOW use an outcomes-based approach.

The outcomes-based approach used to describe the services in this SOW is intended to allow Service Provider the ability to determine the most efficient manner of providing the services so described while achieving all applicable Service Levels; provided that in providing the Services under this SOW the Service Provider complies, at all times, with the Privacy Obligations and the Province Security Policies & Standards (except as specifically agreed otherwise by the Province).

Accordingly, the specific procedures, processes and associated tasks, required to be undertaken by Service Provider to perform the Services under this SOW are not described in this SOW, but will be described more fully in the Security Operating Manual (defined below). As a result, it is the intention of the Parties that Service Provider will do what is required to deliver the Services under this SOW in compliance with the requirements of this SOW, even though the specific procedures, processes and tasks to do so are not specifically identified or otherwise articulated; provided that in doing so the Service Provider shall not be responsible for (or otherwise be required to undertake) those matters that are specified in this SOW or elsewhere in the Transaction Documents as being the responsibility of the Province, a Client or a third party (where the third party is not a Subcontractor of Service Provider for purposes of providing Services under the Agreement).

1.4 Security Operating Manual

For greater clarification, it is the intention of the Parties that the specific procedures, processes, tasks and functions not described in this SOW that are required to be performed by Service

Provider in order to deliver the Services under this SOW shall be described in detail in an operating manual (the "**Security Operating Manual**"), to be prepared by Service Provider as part of the transformation activities under the Transformation SOW. The Security Operating Manual shall form part of the Manual described in Sections 4.8 (*Documentation*) and 4.9 (*Manual Requirements*) of the Agreement. Service Provider will provide the Province with a copy of the Security Operating Manual upon request from time to time.

The Parties acknowledge that on the Hand-Over Date, the Security Operating Manual shall consist of the processes, procedures (and associated tasks and functions) that are in use by the Province immediately prior to the Hand-Over Date (the "**Province Security Procedures**") until the Province Security Procedures have been revised by Service Provider as set forth in the Transformation SOW. The Parties acknowledge that the Province Security Procedures are in various states of completion and drafting, and will not necessarily articulate all processes, procedures, tasks and functions that will be required for Service Provider to provide the Services under this SOW immediately following the Hand-Over Date.

2. GENERAL RESPONSIBILITIES

Prior to Transformation and prior to implementation of required security projects through the Change Order and Change Management processes, the security level and compliance of the Supported Environment as at the Hand-Over Date will be maintained by the Service Provider, at a level of security and compliance that is no less than that provided by the Province on the Hand-Over Date.

2.1 Security Policy and Control Standards Compliance

	Responsibility (R)	
Security Policy and Control Standards Compliance	Province	Service Provider
Provide the list of Province Security Policies & Standards and communicate changes to the Province Security Policies & Standards to Service Provider.	R	
At the request of the Province, implement specified changes to the Province Security Policies & Standards through the Change Order Process.		R
Within 6 months of the Hand-Over Date, perform initial Policy Compliance Manager ("**PCM**") scan on the Initial Supported Infrastructure Servers to determine the level of compliance with the Province Security Policies & Standards, and provide the Province a report on the results of that scan (the "**Initial Policy Compliance Report**").		R
Determine, and communicate to the Service Provider, any remediation priorities on the Initial Policy Compliance Report.	R	

Security Policy and Control Standards Compliance	Responsibility (R)	
	Province	Service Provider
In consultation with the Province, develop remediation plans to address the Province's remediation priorities based on the Initial Policy Compliance Report, and implement through the Change Order Process.		R
Provide an annual report to the Province on the level of compliance of the Initial Supported Infrastructure Servers that have not been Transformed with the Province Security Policies & Standards (the "**Annual Policy Compliance Report**").		R
Determine, and communicate to Service Provider, any remediation priorities on the Initial Policy Compliance Report.	R	
In consultation with the Province, develop remediation plans to address the remediation priorities provided by the Province based on the Annual Policy Compliance Report, and implement through the Change Order Process.		R
Except where otherwise agreed between the Parties, the Supported Infrastructure in the STMS Data Centres will be compliant with the Province Security Policies & Standards.		R
Regardless of location and except as otherwise agreed by the Parties, any new components of the Supported Infrastructure or Transformed components of the Initial Supported Infrastructure, will comply with the Province Security Policies & Standards, or be the subject of an exception, as documented through the Change Management Process.		R
For break fix replacement of non-functioning, non-Transformed Servers in the existing Province Midrange Facilities, replacement of such Servers will utilize the existing Province backup image until the Server is Transformed.		R

2.2 Security Threat and Risk Assessment (STRA)

Security Threat and Risk Assessment (STRA)	Responsibility (R)	
	Province	Service Provider
Implement changes to the Security Threat & Risk Assessment Methodology attached as Appendix C through the Change Order Process.	R	

Security Threat and Risk Assessment (STRA)	Responsibility (R)	
	Province	Service Provider
Conduct STRA for the Supported Infrastructure and the Services, as required by the Province Security Policies & Standards, and upon request, provide the results to the Province.		R
The STRA for the Services and the Supported Infrastructure will include the assessment of risk introduced by any Service Provider supporting infrastructure or systems utilized by Service Provider to access, operate, maintain or manage the Supported Infrastructure.		R
In consultation with the Province, perform STRA for changes to the Supported Infrastructure or the Services (such as changes in architecture, new operating system versions, major service pack updates, changes to the type of security controls/devices/software used), during the planning and design phase of such proposed changes and before implementation.		R
Prior to migrating any Supported Infrastructure to the new STMS Data Centres, complete STRAs on the STMS Data Centre and provide STRA reports to the Province.		R
Review risks identified in each STRA report and, in consultation with the Province, formulate risk mitigation plans.		R
Implement risk mitigation plans through the Change Management Process, or where agreed to by the Parties, through the Change Order Process, and if the Parties are not able to agree on whether or not the Change Order Process applies, then the matter will be escalated through the Governance Process.		R

2.3 Human Resources Security

Service Provider will perform a CRC on Service Provider Personnel directly involved in the delivery of the Supported Infrastructure and having authorized access to personal information under the Agreement. All Transitioning Employees (as defined in the Master Services Agreement) are exempt from the CRC requirements unless the position they fill required a CRC on the Hand-Over Date.

Human Resources Security	Responsibility (R)	
	Province	Service Provider
Perform a CRC on all Service Provider Personnel who may have direct or indirect access to Personal Information before any such access is given, unless specifically approved otherwise by the Province.		R
Investigate all positive results obtained from a CRC in respect of any Service Provider Personnel, and in consultation with the Province address any such positive results before providing such Service Provider Personnel with direct or indirect access to Personal Information.		R

2.4 Cryptographic Key Management

Cryptographic Key Management	Responsibility (R)	
	Province	Service Provider
Provide Service Provider with S15 S15	R	

2.5 Service Provider Personnel Privileged Logical Access to the Supported Infrastructure

2.5.1 Secure Access Gateway Services for Service Provider Personnel ("SP SAG")

Formal procedures for granting and managing logical access to the Supported Infrastructure will be documented and followed. Access authorization (rules for granting access), access establishment (rules that determine initial right of access), access modification (rules that determine the types of, and reasons for, modification to the initial right of access), and access termination (rules that determine the points at which and reasons for which termination of rights of access occurs) are also included in these procedures.

The Privileged ID access control services for Service Provider Personnel will be provided through the SP SAG in accordance with the following table:

Secure Access Gateway Services for Service Provider Personnel (SP SAG)	Responsibility (R)	
	Province	Service Provider
Operate, maintain and manage a Secure Access Gateway to provide controlled access for Service Provider Personnel S15 S15 for purposes of performing the Services.	R	
Implement Service Provide S15 S15		
The SP SAG will be located in the Service Provider S15 S15		R
Review SP SAG Servers S15 for evidence of misuse or abuse of privileges by Service Provider Personnel.	R	
Implement and document processes and procedures to manage and control all accesses to the Supported Infrastructure which are made available to Service Provider Personnel for the purpose of performing the Services.		R
For each requirement that arises for Service Provider Personnel to access or manipulate the Province production data, obtain prior formal written non-transferable approval from the Province.		R
Document, implement and maintain security controls to monitor and grant appropriate access privileges to authorized third parties in accordance with the Province Security Policies & Standards.		R
Assign a Service Provider security administrator for each component of the Supported Infrastructure (such as firewalls, Servers, Host Servers, Virtual Servers and routers).		R
Implement and document processes and procedures to manage, monitor and restrict accesses to the security software and access control mechanism of the Supported Infrastructure to the Service Provider security administrator.		R
Implement and document processes and procedures to revoke all access to the Supported Infrastructure for Service Provider Personnel whose job function no longer requires access to the Supported Infrastructure.		R
Immediately revoke access to Supported Infrastructure upon termination of Service Provider Personnel.		R
Implement and document processes and procedures to prevent direct outside access or connectivity to the Supported Infrastructure in STMS Data Centres.		R

Secure Access Gateway Services for Service Provider Personnel (SP SAG)	Responsibility (R)	
	Province	Service Provider
Implement and document processes and procedures to require that all remote administration activities are performed by Service Provider on the Supported Infrastructure are done through the SP SAG.		R
Implement and document processes and procedures to require that all files transferred into the Supported Infrastructure will only be transferred through the SP SAG. This is not applicable to management toolset file transfer requirements (detailed in section 5.7 (*Direct Device Management*) Device management infrastructure traffic of this SOW and of the Storage and Backup SOW).		R

2.5.2 Service Provider Support and Maintenance Staff – Remote Access

Service Provider Personnel utilizing Remote Access to access the Supported Infrastructure will only do so from a location within Canada S. 15 . The obligations in the table below will be phased in during the first six months following the Hand-Over Date, as documented in the Transformation SOW.

Service Provider Support and Maintenance Staff – Remote Access	Responsibility (R)	
	Province	Service Provider
Service Provider Personnel will use the Service Provide S15 to connect to Service Provider Network and remotely provide support to the Supported Infrastructure.		R
Maintain a minimum level of S15 for all data transported between the Service Provider Personnel devices (such as laptops) and Service Provider Network.		R
Implement and document processes and procedures to require that remote access to the Supported Infrastructure only be allowed using Service Provider issued devices.		R

2.6 Centralized Security Log Collection, Review and Monitoring

Centralized Security Log Collection, Review and Monitoring services is comprised of the collection of security log files for the Supported Infrastructure into a central repository, the implementation of monitoring of the consolidated log files for suspicious activity and the generation of alerts for Service Provider review and intervention. From the Hand-Over Date until

the completion of the STMS Data Centres, Service Provider will perform this service in the same manner as previously performed by the Province prior to the Hand-Over Date.

Security Events monitoring is performed on security log data generated from the Supported Infrastructure.

Tasks and Functions described in the table below, where noted, will become available after the implementation of the new STMS Data Centres.

	Responsibility (R)	
Centralized Security Log Collection, Review and Monitoring	**Province**	**Service Provider**
Enable, implement, configure, maintain, and manage logging on all Supported Infrastructure to levels of detail set forth in the Province Security Policies & Standards commencing after implementation of the new STMS Data Centres.		R
S. 15		R
Retain original content of the Supported Infrastructure Security reports S. 15		R
S. 15		R
S. 15 S. 15 Otherwise, Service Provider to perform this Task/Function commencing after implementation of the new STMS Data Centres.		R
Upon request and in consultation with S. 15 S. 15 Security Incidents and Security Investigations.		R
Upon request and in consultation with the Province using resources assigned to the account S15 S15 for use in Security Incidents and Security Investigations.		R
Upon request and in consultation with the Province, provide the archived security logs in a form that is readable and capable of being copied for use in Security Incidents and Security Investigations.		R

Centralized Security Log Collection, Review and Monitoring	Responsibility (R)	
	Province	Service Provider
Provide S15 that are part of the Supported Infrastructure in original format for analysis by the Province using the Province's tools.		R
Establish, maintain and monitor controls S. 15 S. 15 S. 15 for the Supported Infrastructure.		R
S. 15 , to the Province, as requested through the Change Order Process.		R
Install, configure and maintain centralized logging that supports standard S15 prior to moving any Province data to the new STMS Data Centre.		R
Configure all Supported Infrastructure for logging to S15 implementation.		R
Logically separate log data from other data in the STMS Data Centre.		R
Use Transport Layer Security (TLS) to encrypt communications between the S15		R
Store log files in S. 15		R
Install, configure and maintain S15 on Supported Infrastructure Servers.		R
Install, configure and maintain S15 on the Supported Infrastructure Servers so that it will generate alerts 24x7x365; monitor such alerts as set forth in this SOW.		R

2.7 Investigation and Response to Security Incidents, Compromises and Breaches

2.7.1 Security Incident Response and Handling

Security Incident Response and Handling provides timely and orderly response to information Security Incidents.

Security Incident Response and Handling	Responsibility (R)	
	Province	Service Provider
Provide the Province with a direct point of contact, who will participate and interact with the Province's "Security Incident Response Team" in the event of Province declared Security Incidents.		R
Cooperate and work with the Province to resolve Province declared Security Incidents.		R
Provide the Service Provider with a direct point of contact for the Province's "Security Incident Response Team" to work with the Service Provider in the event of Service Provider declared Security Incident.	R	
Cooperate and work with the Service Provider to resolve Service Provider declared Security Incidents.	R	
Provide a single point of contact for the Province to report Security Incidents and request assistance related to the Security Incidents.		R
Provide a single point of contact for the Service Provider to report Security Incidents and request assistance related to the Security Incidents.	R	
Identify, monitor, investigate and resolve Security Incidents.		R

2.7.2 Security Investigations

Security Investigations provides in-depth, technical analysis and technical investigative work to determine the cause and the effect and impact on the Supported Infrastructure of the Security Incident. This service will include computer forensics work, as deemed appropriate during the investigation.

Security Investigations	Responsibility (R)	
	Province	Service Provider
Interact with third-party vendors as necessary to determine root cause analysis of Security Incidents.		R
Maintain Security Incident information and documentation on investigations undertaken by the Service Provider in accordance with Service Provider standards (for a minimum of one year) for handling sensitive information.		R

Security Investigations	Responsibility (R)	
	Province	Service Provider
Conduct Security Investigations and perform root cause analysis where necessary on Security Incidents relating to the Supported Infrastructure.		R
Provide the Province with Security Investigation findings that are relevant to the Services or the Supported Infrastructure.		R
Service Provider will provide support to the Province's Security Investigation efforts.		R
Upon request by the Province, provide the Province's investigators with the required logical and physical access to the Supported Infrastructure while conducting a Security Investigation, which access will be provided in accordance with a process to be mutually agreed upon by the Parties within six months of the Hand-Over Date.		R
Provide a direct point of contact for Security Investigations that can be used by the Province.		R
Security breaches, compromises or data loss detected or identified by Service Provider will be escalated to the Province in accordance with the Security Operating Manual S. 15 S. 15		R
The Province will provide a direct point of contact for Security Investigations that can be used by Service Provider.	R	
Implement and maintain processes and procedures so that data evidence collection, preservation and chain of custody are maintained.		R
Implement processes and procedures to obtain permission from the Province prior to analyzing forensic images containing Province data.		R
Provide Service Provider with information from the Province Systems relating to Service Provider Security Investigations.	R	
Provide the Province with the current Master Virtual Image of servers in support of investigations involving Virtual Servers.		R
Provide the Province with S. 15 S. 15		R
In instances where storage for requested Virtual Images is not available, notify and work with the Province to identify workaround for storage of requested Virtual Images.		R

Security Investigations	Responsibility (R)	
	Province	Service Provider
S. 15		R
Provide the Province with access and/or possession (including removal if required) of Supported Infrastructure Servers when required by Court Order or other judicial or legal proceedings, pursuant to the Change Order Process.		R
S. 15 as reasonably required to support Province Security Investigation.		R

2.8 Annual Security Health Check

The scope of the Annual Security Health Check covers the Supported Infrastructure.

Annual Security Health Check	Responsibility (R)	
	Province	Service Provider
Complete Annual Security Health Check, by the end of S15 Provide the results to the Province no later that S15		R
Communicate to Service Provider by S15 the current Annual Security Health Check methodology and the designated procedure for completion/submission of reports as defined by the Province.	R	
Implement changes to the Annual Security Health Check methodology through the Change Order Process.		R

3. MAINFRAME SECURITY SERVICES

3.1 Secure Mainframe Access – S15

Secure Mainframe Access - S15 Access provides user Local Area Network (LAN) workstations with secure communications connectivity access from a workstation to a mainframe host.

Secure Mainframe Access – TN3270e	Responsibility (R)	
	Province	Service Provider
Provide secure access to the Service Provider mainframe using S15		R
Acquire, manage and administrate digital certificates for the S15 S15		R
Provide identification / authentication mechanisms, using an encryption standard consistent with the Province Security Policies & Standards.		R

3.2 File Transfer Protocol with Secure Socket Layer / Transport Layer Security (FTPS SSL/TLS)

Secure FTPS SSL / TLS service provides a secure, encrypted communication path between workstations, Servers, Client Server Applications and the Mainframe System.

File Transfer Protocol with Secure Socket Layer / Transport Layer Security (FTPS SSL/TLS)	Responsibility (R)	
	Province	Service Provider
Provide secure access to the Mainframe System using FTPS communication protocol over SSL / TLS.		R
Provide identification / authentication mechanisms using an encryption standard consistent with the Province Security Policies & Standards.		R
Acquire and manage the life cycle, retention and renewal of digital certificates for the SSL / TLS FTPS service.		R

3.3 Secure Shell File Transfer Protocol (SFTP)

Secure Shell SFTP (SSH) Access provides a secure, encrypted communication path between workstations, Servers Client Server Applications and the Mainframe System.

Secure Shell File Transfer Protocol (SFTP)	Responsibility (R)	
	Province	Service Provider
Provide secure access to the Mainframe System using SFTP/ (SSH) communication protocol.		R

Secure Shell File Transfer Protocol (SFTP)	Responsibility (R)	
	Province	Service Provider
Provide identification / authentication mechanisms and encryption consistent with the Province Security Policies & Standards.		R
Acquire and manage the life cycle, retention and renewal of digital certificates for the SFTP (SSH).		R

3.4 Digital Certificate Administration Mainframe

Digital Certificate Administration Mainframe provides a Digital Certificate management service in support of the secure connections capabilities.

Digital Certificate Administration Mainframe	Responsibility (R)	
	Province	Service Provider
S. 15 for creation of digital certificates.	R	
Provide required digital certificate if and when requested.		R
Notify of pending expiration of digital certificates.		R
Provide request to Service Provider to implement Digital Certificates.	R	
Respond to vendor notification of pending expiration of digital certificate, with request for re-issued certificate, if appropriate.		R

3.5 Mainframe Security Administration

The Province is responsible for the architecture oversight, implementation, and day to day operation of Mainframe Security. Service Provider has specific responsibilities as delegated by the Province as set forth in this section. Mainframe Security Administration has been implemented in the Province as a distributed model, whereby each organization (Province, Ministry, Broader Public Sector, or vendor) is responsible for Security Administration within their scope of control.

Mainframe RACF Administration	Responsibility (R)	
	Province	Service Provider
Install, maintain, upgrade and support the Security System Software and access management databases S. 15 on the Mainframe System.		R

Mainframe RACF Administration	Responsibility (R)	
	Province	Service Provider
Verify and support data integrity protection software options that have been implemented on the Mainframe System by the Province.		R
Process authorized requests to create, delete or change a Mainframe System user identification through the Change Management Process.	R	
Provide Government Data Security Access ("**GDSA**") (as defined in the Mainframe SOW) services for Service Provider S. 15 S. 15		R
Process authorized requests to change Service Provider S. 15 S. 15		R
Install and verify all security exits implemented and as developed by the Province. Inform the Province upon completion.		R
S. 15		R
Obtain Province approval prior to implementing or modifying configuration parameters that may affect Mainframe System security (RACF) S. 15		R
Provide subject matter expertise, recommendations and assistance to the Province in defining and implementing special access profiles on the Mainframe System (e.g., Program Access to Data Sets (PADS)).		R

4. MIDRANGE SECURITY SERVICES

4.1 Security Administration and Compliance Services

Service Provider will provide Security Administration and Compliance Services by configuring "Midrange" Supported Infrastructure in accordance with the Province Security Policies & Standards.

Security Administration and Compliance Services	Responsibility (R)	
	Province	Service Provider
Develop and implement processes and procedures to provide privileged IDs during Change Windows to those Province users who have authorized Change Control Board activities to perform and to revoke such privileges at the end of the Change Window.		R

Security Administration and Compliance Services	Responsibility (R)	
	Province	Service Provider
Develop and implement processes and procedures to control the creation of Administrative Support IDs and the assignment of privileges to those IDs.		R
Develop and implement processes and procedures to detect unauthorized configuration changes in the Midrange Supported Infrastructure.		R

4.2 Policy Compliance Management Services

Policy Compliance Management (PCM) Services manages the automated process of gathering security configuration information from Servers. S. 15

S. 15

Policy Compliance Management Services	Responsibility (R)	
	Province	Service Provider
Install and maintain software and hardware as necessary to support PCM service.		R
Manage the Province's network (SPAN/BC) rule changes to support the PCM service.	R	
Inform the Province of firewall or router ACL rule changes to the Province network (SPAN/BC) required to enable the PCM service.		R
S. 15		R
Provide necessary approvals for performing PCM related activities as requested.	R	
S. 15		R

4.3 Vulnerability Scanning Service

The Vulnerability Scanning Service supports compliance with the Province Security Policies & Standards, by S. 15

S. 15

Vulnerability Scanning Service	Responsibility (R)	
	Province	Service Provider
Perform a vulnerability scan S. 15 S. 15		R
Perform remediation identified by vulnerability scans S. 15 S. 15 and notify the Province through the Change Management Process, where applicable.		R
Maintain the currency of the scanning tool.		R
Provide authorization to perform the vulnerability scan.	R	
If the Province's vulnerability scans on the Supported Infrastructure in the STMS Data Centre S. 15 S. 15 through the Governance Process.	R	
If the Service Provider S. 15 S. 15 the Service Provider may raise this matter with the Province, and they will resolve it through the Governance Process.		R

4.4 Vulnerability and Security Patch Management

Vulnerability and Security Patch Management consists of the deployment and management of Security patches as required by Province Security Policies & Standards S. 15 S. 15 for the Supported Infrastructure.

Vulnerability and Security Patch Management	Responsibility (R)	
	Province	Service Provider
In compliance with the Province Security Policies & Standards, establish and maintain vulnerability management practices, S. 15 S. 15 S. 15 as described in the Service Management SOW.		R

Vulnerability and Security Patch Management	Responsibility (R)	
	Province	Service Provider
When a security vulnerability S. 15 S. 15 S. 15		R
Based on vulnerability S. 15 S. 15	R	

4.5 Anti-virus and Anti-spyware Services

The Anti-virus and Anti-spyware Services provides protection S. 15
The anti-virus service is comprised of the following:

Anti-virus and Anti-spyware Services	Responsibility (R)	
	Province	Service Provider
Develop and implement processes and procedures to maintain currency of anti-virus software on the Servers.		R
Utilize the Service Provider's S. 15 S. 15		R
Troubleshoot and resolve problems associated with the S. 15 S. 15		R
Subscribe to and monitor services S. 15 S. 15 with the Province as described in the Security Operations Manual.		R
Monitor and initiate S. 15 S. 15		R
Provide a single point of contact for confirmed virus outbreaks.		R

4.6 Configuration Control

Configuration Control consists of the development and implementation of security controls relating to configuration changes to the "Midrange" Supported Infrastructure as set forth below and in the Service Management SOW.

Configuration Control	Responsibility (R)	
	Province	Service Provider
Develop and implement processes & procedures S. 15 S. 15 S. 15 in accordance with the Province's Security Policies & Standards.		R
S. 15 for configuration changes to the Midrange Supported Infrastructure.		R

5. NETWORK SECURITY SERVICES

The security architecture of the STMS Data Centre is illustrated in Diagrams in Appendix D. Service Provider will implement controls around changes to the security architecture as described below.

Network Security Services	Responsibility (R)	
	Province	Service Provider
Develop, implement and maintain processes, procedures and controls to ensure that there is no direct internet connection into the STMS Data Centre network.		R
Configure security architecture of the STMS Data Centre in accordance with Appendix D.		R
Develop, implement and maintain processes, procedures and controls to ensure changes to the security controls that support the security architecture in the STMS Data Centres are documented and approved by the Province prior to implementation.		R

5.1 Data Centre Network Security Architecture Design

Service Provider will construct the STMS Data Centres in accordance with the technical architecture depicted in Appendix D, unless otherwise agreed by the Parties

5.2 Firewall Service

The Firewall Service includes all firewalls in the STMS Data Centre.

These firewalls S. 15 S. 15

Firewall Service	Responsibility (R)	
	Province	Service Provider
Provide firewall hardware and software for the STMS Data Centre.		R
Provide firewall administration, maintenance and management and associated rule configuration changes.		R
Provide firewall S. 15 monitoring of S. 15 S. 15 Perform S. 15 firewall monitoring S. 15 S. 15 on a 24 hours a day, 7 day per week, 365 days per year ("24x7x365") basis. S15 S15		R
Develop, implement and maintain processes and procedures to generate alerts to Service Provider through an automated process integrated with the S15		R
Implement up to an aggregate S22 Province- initiated rule changes as determined by the Province.		R
Develop, implement and maintain processes and procedures to fully S. 15		R
Restore firewall configurations as required.		R

5.3 Intrusion Prevention Service

The Intrusion Prevention Service includes all intrusion prevention systems in the STMS Data Centre.

The Intrusion Prevention Service (IPS) S. 15 S. 15

Intrusion Prevention Service	Responsibility (R)	
	Province	Service Provider
Provide IPS hardware and software for the STMS Data Centre.		R
Provide IPS administration, maintenance and management and associated rule configuration/changes.		R
Provide IPS S. 15 monitoring S. 15 S. 15 .		R

Intrusion Prevention Service	Responsibility (R)	
	Province	Service Provider
Perform remote S. 15 IPS monitoring S. 15 on a 24 hours a day, 7 day per week, 365 days per year ("24x7x365") basis. S15 S15		R
Develop, implement and maintain processes and procedures to generate alerts to Service Provider through an automated process integrated with th S15		R
Implement up to an aggregate S15 per IPS S15 Province. Province- initiated rule changes as determined by the		R
Develop, implement and maintain processes and procedures to S. 15 S. 15		R
Restore IPS configurations as required.		R

5.4 Managed LAN/Router Services

Managed LAN/Router Services refers to switches and routers used in the STMS Data Centre.

Managed LAN/Router Services	Responsibility (R)	
	Province	Service Provider
S. 15		R
Implement strong access controls and centralized authentication S. 15 S. 15 to all switches and routers in the STMS Data Centre.		R

5.5 WAN

The security architecture of the STMS Data Centre is illustrated in Diagrams in Appendix D. Service Provider will implement controls around changes to the security architecture as described below.

WAN connectivity for the STMS Data Centre is detailed in architecture diagram 5 in Appendix D.

WAN	Responsibility (R)	
	Province	Service Provider
Provide private WAN connectivity S15 dedicated to the interconnection of the Supported Infrastructure.		R
Configure WAN connectivity between the STMS Data Centres in accordance with Appendix D.		R
Develop, implement and maintain processes, procedures and controls so that all changes to the security controls that support the WAN connectivity between the STMS Data Centres are documented and approved by the Province prior to implementation.		R

5.6 Province Owned Security Devices/Controls

The Province will require the ability to place Province owned security devices in the STMS Data Centre, S. 15

Province Owned Security Devices/Controls	Responsibility (R)	
	Province	Service Provider
Install, maintain and support Province owned security devices in the STMS Data Centre in accordance with the terms agreed through the Change Order Process.		R

5.7 Direct Device Management

Some Service Provider S. 15 will require direct access S. 15 and will not go through the S. 15 S. 15 Such accesses will be handled as described below.

Direct Device Management	Responsibility (R)	
	Province	Service Provider
Configure all accounts used for direct access of Service Provider's management S. 15 S. 15		R
Restrict all direct access of Service Provider's S. 15 S. 15		R

Direct Device Management	Responsibility (R)	
	Province	Service Provider
Limit all direct access of Service Provider's S. 15 S. 15		R

5.8 Virtual Local Area Networks

Service Provider will implement Virtual Local Area Networks (VLANs) within the STMS Data Centre as described in the following table.

Virtual Local Area Networks	Responsibility (R)	
	Province	Service Provider
Configure VLANs S. 15 S. 15		R
Configure VLANs securely S. 15 S. 15		R

6. STORAGE SECURITY SERVICES

6.1 Storage Area Network (SAN) Security Configuration

Storage Area Network (SAN) Security Configuration services provides protection against unauthorized access S. 15 These services will be implemented in accordance with the schedule for implementation of the SAN set forth in the Transformation SOW.

Storage Area Network (SAN) Security Configuration	Responsibility (R)	
	Province	Service Provider
Provide SAN Security hardware and software for the Supported Infrastructure.		R
Implement and manage strong access control S. 15 S. 15		R
Provide SAN Security administration, maintenance and management and associated configuration changes.		R

7. DATA ENCRYPTION SERVICES

7.1 Backup Tape Encryption

The Service Provider Backup Tape Encryption Services will configure S. 15 S. 15 The Backup Tape encryption services will include the following:

	Responsibility (R)	
Backup Tape Encryption	Province	Service Provider
Implement S. 15		R
Encrypt S. 15 S. 15		R
Administer key provisioning including all phases of key lifecycle for backup tape encryption.		R
Provision/de-provision keys.		R
Perform encryption key S. 15		R
Provide support and maintenance for issues related to key management system and corresponding devices.		R

7.2 Encryption of data at rest

Service Provider will make available the host operating system encryption features for data at rest.

	Responsibility (R)	
Encryption of data at rest	Province	Service Provider
Install, test and make available S. 15 for use on the Transformed Servers. If, as a result of utilizing S. 15 on the Transformed Servers, there is a cost or service impact, the Parties will resolve the matter through the Governance Process.	R	

8. ADDITIONAL SERVICES

This Article 8 describes a set of additional Services that may be purchased by the Province from Service Provider, performed by and on the Province's own behalf or purchased by the Province through a third party vendor. To the extent they are purchased by the Province from Service Provider, such purchase will be documented through the Change Order Process and they will be deemed included in the definition of "Supported Infrastructure."

To the extent the Province purchases these Services, the Parties will work together to prepare and agree on the Transformation Plan for implementation of such Services.

8.1 Enterprise Security Event Management and Security Incident Response Services

The ESEM services may be purchased as two different tiers of services: (1) 24x7x365 or (2) standard business hours (8:30-4:30 Mon-Fri, not including statutory holidays). The services described below apply to both tiers except where expressly noted otherwise.

8.1.1 Enterprise Security Event Management Services Overview

Enterprise Security Event Management ("**ESEM**") is a service that S. 15 S. 15 ESEM is implemented using an integrated set of processes, personnel, and technologies that supplement other security activities.

The ESEM services provided by Service Provider will consist of the following functions to the extent as described in the table below:

	Responsibility (R)	
Enterprise Security Event Management Services Overview	Province	Service Provider
Test, implement and maintain a dedicated ESEM system in STMS Data Centre or other agreed Service Provider location S. 15 S. 15 S. 15 and other devices as determined by the Province (collectively, the "ESEM Monitored Devices") S15		R
Provide network connectivity to the ESEM Monitored Devices in and connected to the Province network (SPAN/BC).	R	
Configure the ESEM Monitored Devices S. 15 S. 15 ESEM System and provide specifications to the Province for configuration of ESEM Monitored Devices that are managed by the Province.		R

Enterprise Security Event Management Services Overview	Responsibility (R)	
	Province	Service Provider
Configure the ESEM Monitored Devices that are managed by the Province S. 15 S. 15 based on specifications provided by Service Provider.	S. 15	
Make certain that the Province Data continues to be transmitted and can be received within the ESEM Private Security Network S. 15 S. 15	R	

Log Analysis

Log analysis is an automated function that processes collected system logs and security alerts from the ESEM Monitored Devices and compares and correlates that data S. 15 S. 15

Log Analysis	Responsibility (R)	
	Province	Service Provider
Develop and tune thresholds and baselines to be used S. 15 S. 15 of the ESEM Monitored Devices.		R
Approve the ESEM thresholds and baselines to be used for S. 15 S. 15 and proposed changes to those thresholds and baselines.	R	
Develop, implement and maintain processes and procedures to S. 15 to Service Provider based upon the agreed ESEM thresholds and baselines.		R
Review alerts and respond as appropriate, which may include tuning of ESEM thresholds and baselines, Service Management response to the ESEM Monitored Devices, S. 15		R
Provide S. 15 S. 15		R
S. 15		R

Log Analysis	Responsibility (R)	
	Province	Service Provider
S. 15		R

Backup/Restore	Responsibility (R)	
	Province	Service Provider
Develop, implement and maintain processes and procedures to fully backup and restore the ESEM configuration data and data storage directories.		R
Restore ESEM data as requested through Change Order Process.		R

Standard Functions of ESEM Reporting

ESEM reporting allows the Province to receive reports produced from compiled data and information collected by ESEM through a set of preconfigured ESEM reports. Report delivery is restricted to individuals who are authorized by the Province to receive the reports from Service Provider. Available ESEM reports are selected from a preconfigured list of ESEM reports made available by Service Provider to the Province.

Standard Functions of ESEM Reporting	Responsibility (R)	
	Province	Service Provider
Run and produce ESEM reports in the manner and at the specified reporting frequency as established by the parties.		R
Distribute ESEM reports as produced to the authorized Province recipient via email.		R
Define the Province reporting requirements and reporting specifications and communicate such requirements and specifications to Service Provider.	R	
Select the specific preconfigured ESEM reports that will be produced and the frequency that they will be required.	R	
Define and provide to Service Provider appropriate contact information and reporting mechanism (such as e-mail, mailing address, etc.) for delivery of reports.	R	

Standard Functions of ESEM Reporting	Responsibility (R)	
	Province	Service Provider
Notify Service Provider S. 15 if an ESEM report is not received by the approved Province recipient in accordance with the established reporting frequency parameter.	R	

Two Factor Authentication

At the request of the Province through the Change Order Process, Service Provider will implement and maintain a Two Factor Authentication (2FA) for privileged access for Service Provider Personnel, Province Personnel, or both. The two-factor authentication includes:

- RSA Enterprise License S15 S15
- Service Provider administration of the RSA Tokens
- Required security servers and ongoing Service Provider hosting of those servers

Two Factor Authentication	Responsibility (R)	
	Province	Service Provider
Implement and maintain an RSA token based two-factor authentication and associated infrastructure for Service Provider Personnel, Province Personnel, or both to access the Supported Infrastructure.		R
Develop, document and maintain processes and procedures to manage the RSA tokens.		R

8.2 Secure Access Gateway for Province Personnel

The Secure Access Gateway will consist of the Citrix servers and the system administration and maintenance tool set ("**BC SAG**") for Province Personnel to access the Supported Infrastructure.

Secure Access Gateway for Province Personnel (BC SAG)	Responsibility (R)	
	Province	Service Provider
Implement and maintain the BC SAG at one or both of the STMS Data Centres.		R

Secure Access Gateway for Province Personnel (BC SAG)	Responsibility (R)	
	Province	Service Provider
S. 15 and infrastructure used to provide the BC SAG.		R
Implement and document processes and procedures to manage S15 S15 Province Personnel's access to BC SAG.		R

8.3 Payment Card Industry Data Security Standards (PCI DSS) Infrastructure

The PCI DSS Infrastructure is a compartment within the STMS Data Centres that is compliant with the higher of the PCI DSS 1.2 or the Supported Infrastructure Security Policy. The responsibilities in the RASIC table below apply to the Supported Infrastructure within the PCI DSS compartment and the network traffic flow in and out of that compartment. For the purpose of the table that follows, "cardholder data environment" is a term synonymous with the term "PCI DSS Infrastructure."

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
Establish in consultation with the Province, firewall and router configuration standards that include the following: • A formal process for approving and testing all network connections and changes to the firewall and router configurations. • Current network diagram with all connections to cardholder data, including any wireless networks. • S. 15 • S. 15 • Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. • Requirement to review firewall and router rule sets at least S15		R
Provide, and inform Service Provider of, business justification for use of all services, protocols, and ports allowed for application and	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
database components, including documentation of security features implemented for those protocols considered to be insecure.		
In consultation with the Province, S. 15 S. 15 • S15 •		R
In consultation with the Province, prohibit direct public access between the Internet and any system component in the cardholder data environment, by implementing the following controls: S15		R
		R

Pages 278 through 280 redacted for the following reasons:
- -
S15, S15

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
vulnerability		
Follow change control procedures for all changes to infrastructure components by implementing the following procedures: • Documentation of impact • Management sign-off by appropriate parties • Testing of operational functionality • Back-out procedures		R
Follow change control procedures for all changes to application and database components by implementing the following procedures: • Documentation of impact • Management sign-off by appropriate parties • Testing of operational functionality • Back-out procedures	R	
For public-facing web applications, address new threats and	R	

S15

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: S15		
Limit access to infrastructure components and cardholder data to only those individuals whose job requires such access by implementing the following controls: S. 15		R
Limit access to application and database components, and cardholder data, to only those individuals whose job requires such access by implementing the following controls: S. 15	R	
Establish an access control system for infrastructure components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. S. 15		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
S. 15		
Establish an access control system for application and database components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	R	
		R
	R	
		R
S. 15	R	
		R
		R
	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
Ensure proper user authentication and password management for non-consumer users and administrators on all SP PCI infrastructure components as follows: S15		R
consumer users and administrators on all PCI application and database components as follows:	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
S15		
In consultation with the Province, use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment through implementation of the following		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
controls. S15		
In consultation with the Province, develop procedures to help Service Provider easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.		R
Make sure all visitors are handled as follows: S15		R
Use a visitor log to maintain a physical audit trail of visitor activity. S. 15		R
Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. S. 15		R
Establish a process for linking all access to infrastructure components S. 15		R
In consultation with Service Provider, establish a process for linking all application and database component-related access to system	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
components (especially access done with administrative privileges such as root) to each individual user.		
In consultation with the Province, implement automated audit trails for all SP PCI infrastructure components to reconstruct the following events: S15		R
In consultation with Service Provider, implement automated audit trails for all application and database components to reconstruct the following events: S15	R	
Record at least the following audit trail entries for all SP PCI infrastructure components for each event: S15		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
S15		
Record at least the following audit trail entries for all application and database components for each event: S15	R	
Synchronize all critical system clocks and times for SP PCI infrastructure components.		R
Synchronize all critical system clocks and times for application and database components.	R	
Secure audit trails for the SP PCI Infrastructure so they cannot be altered.		R
Secure audit trails for application and database components so they cannot be altered.	R	
S. 15		R
	R	
Protect audit trail files from unauthorized modifications on SP PCI infrastructure components.		R
Protect audit trail files from unauthorized modifications on application and database components.	R	
Promptly back up audit trail files for SP PCI Infrastructure S. 15 S. 15		R
Promptly back up audit trail files for application and database components S. 15 S. 15	R	
Write logs for external-facing technologies such as wireless, firewalls,		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
DNS and mail servers for the SP PCI Infrastructure S. 15 S. 15		
Write logs for external-facing technologies such as wireless, firewalls, DNS and mail servers for Province-managed devices in the Province PCI environment S. 15	R	
Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed S. 15 S. 15		R
Review logs for all system components S. 15 Log reviews must include those servers that perform S15 S15		R
Retain S. 15 S. 15 (for example, online, archived, or restorable from back-up).		R
Test for the presence of wireless access points by using S15 S15		R
Run internal vulnerability scans S15 S15		R
Run external network vulnerability scans S15 S15	R	
Perform internal penetration testing at least S15 S15		R
Perform external penetration testing at least S15 S15	R	
Perform network-layer penetration tests, internal.		R
Perform network-layer penetration tests, external (in consultation with	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
Service Provider).		
Perform application-layer penetration tests (in consultation with Service Provider).	R	
Use intrusion-detection systems, and/or intrusion-prevention systems S15 S15 Keep all intrusion-detection and prevention engines up-to-date.		R
Deploy file-integrity monitoring software S15 S15		R
Establish, publish, maintain, and disseminate a Service Provider security policy that: S. 15		R
Establish, publish, maintain, and disseminate a Province security policy that: S. 15	R	
Develop daily operational security procedures that are consistent with requirements in this specification and applicable to Service Provider Personnel, as defined in this table (for example, user account maintenance procedures, and log review procedures).		R
Develop daily operational security procedures that are consistent with requirements in this specification and applicable to Province Personnel, as defined in this table (for example, user account maintenance procedures, and log review procedures).	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
Develop usage policies for critical Service Provider employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors within the context of the PCI DSS Infrastructure. Ensure these usage policies require the following: • Explicit management approval • Authentication for use of the technology • A list of all such devices and personnel with access • Labeling of devices with owner, contact information, and purpose • Acceptable uses of the technology • Acceptable network locations for the technologies • List of company-approved products • Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity • Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use • When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.		R
Develop usage policies for critical Province employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors within the context of the PCI DSS environment. Ensure these usage policies require the following: • Explicit management approval • Authentication for use of the technology • A list of all such devices and personnel with access • Labeling of devices with owner, contact information, and	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
purpose • Acceptable uses of the technology • Acceptable network locations for the technologies • List of company-approved products • Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity • Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use • When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.		
Ensure that the security policy and procedures clearly define information security responsibilities for all Service Provider Personnel within the context of the PCI DSS Infrastructure.		R
Ensure that the security policy and procedures clearly define information security responsibilities for all Province employees and contractors within the context of the PCI DSS environment.	R	
Within the context of the PCI DSS Infrastructure, assign to an individual or team the following Service Provider information security management responsibilities: • Establish, document, and distribute security policies and procedures. • Monitor and analyze security alerts and information, and distribute to appropriate personnel. • Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. • Administer user accounts, including additions, deletions, and modifications • Monitor and control all access to data.		R
Within the context of the PCI DSS environment, assign to an individual or team the following Province information security	R	

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
management responsibilities: • Establish, document, and distribute security policies and procedures. • Monitor and analyze security alerts and information, and distribute to appropriate personnel. • Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. • Administer user accounts, including additions, deletions, and modifications • Monitor and control all access to data.		
Within the context of the PCI DSS Infrastructure, Implement a formal security awareness program to make all Service Provider employees supporting the hosting environment aware of the importance of cardholder data security. • Educate employees upon hire S. 15 • Require employees to acknowledge S. 15 that they have read and understood the company's security policy and procedures.		R
Within the context of the PCI DSS environment, Implement a formal security awareness program to make all Province employees aware of the importance of cardholder data security. • Educate employees upon hire S. 15 • Require employees to acknowledge S. 15 that they have read and understood the company's security policy and procedures.	R	
		R
S. 15	R	
Where Service Provider is permitted by the Province to share cardholder data with "service providers" (as the term is used in the		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
DSS glossary in Appendix A.1), maintain and implement policies and procedures to manage "service providers," to include the following: • Maintain a list of "service providers." • Maintain a written agreement that includes an acknowledgement that the "service providers" are responsible for the security of cardholder data the "service providers" possess. • Ensure there is an established process for engaging "service providers" including proper due diligence prior to engagement. • Maintain a program to monitor "service providers" PCI DSS compliance status.		
If cardholder data is shared with "service providers"' by the Province, maintain and implement policies and procedures to manage service providers, to include the following: • Maintain a list of "service providers." • Maintain a written agreement that includes an acknowledgement that the "service providers" are responsible for the security of cardholder data the "service providers" possess. • Ensure there is an established process for engaging "service providers" including proper due diligence prior to engagement. • Maintain a program to monitor "service providers'" PCI DSS compliance status.	R	
Within the context of the SP PCI DSS Infrastructure, implement an incident response plan to respond immediately to a system breach.		R
Within the context of the PCI DSS environment, implement an incident response plan to respond immediately to a system breach.	R	
Within the context of the SP PCI DSS Infrastructure, create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication strategies in the event of a compromise including notification of payment brands, at a minimum		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
• Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses for all critical system components • Reference or inclusion of incident response procedures from the payment brands		
Within the context of the PCI DSS environment, create the incident response plan to be implemented in the event of application or database-component breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication strategies in the event of a compromise including notification of payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises • Coverage and responses for all critical system components • Reference or inclusion of incident response procedures from the payment brands	R	
Within the context of the PCI DSS Infrastructure, S15 S15		R
Within the context of the PCI DSS environment Compartment S15 S15	R	
Within the context of the PCI DSS Infrastructure, designate specific Service Provider Personnel to be available on a 24/7 basis to respond to alerts.		R
Within the context of the PCI DSS environment, designate specific Province personnel to be available on a 24/7 basis to respond to alerts.	R	
Within the context of the PCI DSS Infrastructure, provide appropriate training to Service Provider Personnel with security breach response responsibilities.		R

Payment Card Industry Data Security Standards (PCI DSS) Infrastructure	Responsibility (R)	
	Province	Service Provider
Within the context of the PCI DSS environment, provide appropriate training to Province staff with security breach response responsibilities.	R	
Within the context of the PCI DSS Infrastructure, include infrastructure alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.		R
Within the context of the PCI DSS e Write logs for external-facing technologies onto a log server on the internal LAN environment, include application and database alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	R	
Within the context of the PCI DSS Infrastructure, develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.		R
Within the context of the PCI DSS environment, develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	R	

Appendix A – Definitions

Term	Definition
Annual Policy Compliance Report	A report outlining the changes to the Province policies in the previous year and the Service Provider actions taken to address those changes as well as those changes the Province would require the Service Provider to address through change control.
Annual Security Health Check	The yearly self-assessment of the state of security across the Province's various information technology platforms and environments. On completion, a report indicating the ranking (currently on a scale of 1 to 5) of the effectiveness of security in a number of defined areas is produced to assist government in evaluating the state of security and areas to focus on for improvement. As indicated in this SOW, the Province's methodology may be amended from time to time through the change control process. The current assessment is accomplished through various assessment questionnaires that will be provided to the Service Provider and may be validated through audits. The assessment questionnaires will be provided through standardized tools that may include but are not limited to: paper forms; electronic documents; or online web forms. These assessments may change over time as governmental policy and standardized tools change. The current standard for security policy compliance assessment is completion of the International Security Forum (https://www.securityforum.org/index.htm) Security Health Checklist.
CRC	Means, either: (a) a Government of Canada Reliability Status clearance a CRC; or (b) a search of applicable criminal records indicating (1) Convictions (indictable offences in the past five years, does not include pardoned records) and summary conviction offences in the past three years); (2) Specific sentences (absolute discharges in the past one year), conditional discharges in the past three years), and stays of proceedings in the past one year); (3) Alternative Measures / Extrajudicial Sanctions (first time involvement

Term	Definition
	reported for one year, and any multiple involvements that are disclosed as a component of information contained in police files); (4) Pending / Outstanding Charges; (5) Outstanding Warrants; (6) Not Criminally Responsible – Mental Disorder; (7) Pardons (no information disclosed concerning pardoned offences); (8) Court Orders (disclosed for the duration of the court order); and (9) Police Files / Information.
Initial Policy Compliance Report	Report resulting from the first Policy Compliance Manager (PCM) tool scan of the supported infrastructure servers.
Initial Supported Infrastructure	The Supported Infrastructure as it exists on the Hand-Over Date.
Master Virtual Image	The image/build of the OS of the physical system/server running one or multiple instances of a software implementation of a hardware-like architecture, which executes predefined instructions in a fashion similar to a physical central processing unit (CPU). A Virtual Image can be used to create a cross-platform computing environment that loads and runs on computers independently of their underlying CPUs and operating systems.
Privileged ID	System ID used by Privileged Users to authenticate to a computer system providing those users with access rights above those of the user population.
Privileged User	Means a user with allocated powers within the Supported Infrastructure which are significantly greater than those available to the majority of users and include systems administrators, network administrators and database administrators. Responsibilities include keeping the systems available, and may include rights to create new user profiles, add or change the privileges and access rights of existing users or take authorized action which may affect computing systems, network communication, or the accounts, files, data, or processes or other users.
Mainframe	A large-capacity computer system with processing power that is significantly superior to PCs or midrange

Term	Definition
	computers.
Province Personnel SAG	Means Secure Access Gateway providing privileged access to the Supported Infrastructure by Province Personnel.
Province Security Policies & Standards	The security policies and standards established by the Province and amended from time to time. At the Hand-Over Date, the Province Security Policies & Standards consist of the following documents: • **Core Policies and Procedures Manual (CPPM) and CPPM Chapter Supplemental** (all applicable chapters, and especially chapter 12 and chapter 12 Supplemental, 14, 15, 16, 20) http://www.cio.gov.bc.ca/legislation/policy/default.asp • **Information Security Policy** http://www.cio.gov.bc.ca/legislation/policy/default.asp • **Records Management Policies** http://www.cio.gov.bc.ca/legislation/policy/default.asp • **IM/IT Standards Manual** http://www.cio.gov.bc.ca/legislation/standards/default.asp • **IT Asset Disposal Standards** http://pss.gov.bc.ca/air/disposal-handbook.html • **Physical Security Standards** • **Security Enhancement Project Architecture Document**
Province Systems	The information technology infrastructure which connects the Service Provider Supported Infrastructure to the Province as well as the Province owned and managed monitoring and security systems, including without limitation items such as switches, routers, firewalls, intrusion prevention/detection systems, domain name servers, domain controllers and security incident and

Term	Definition
	event management systems.
Remote Access	Connection to the Supported Infrastructure which traverses a network that is not under the direct control of the Province or the Service Provider.
Secure Access Gateway (SAG)	A secure application access solution that provides administrators granular application-level control while empowering users with access from anywhere. It gives IT administrators a single point of control to manage access and actions based on both the user and the endpoint device, providing better risk, security and compliance management.
Security Event	Any event that attempts to change the security state or violate the security policy of a system (for example, change the security level of the subject, change a user's password, too many attempts to log on, attempts to violate the limits of a device, attempts to downgrade the classification of a file, and so on).
Security Event Logging	A detective control that enables the recording of Security Events on the Supported Infrastructure based on preset parameters. The administrative tool's logging function is enabled and the Security Events are retained in a record for future review.
Security Incident	Occurs whenever information is compromised, when there is a risk for compromise of information, when recurring potential, successful, or unsuccessful attempts to obtain unauthorized access to a system are detected, or where misuse or abuse of the system is suspected.
Security Investigation	The formal process of inquiring into a Security Incident through research, follow-up, study or formal procedure of discovery to determine the root cause of a Security Incident.
Service Provider Network	A robust, state-of-the-art network that connects Province Clients to Service Provider Services, providing a platform for improved end-to-end service quality, performance visibility, security and service delivery.

Term	Definition
Service Provider SAG	Means Secure Access Gateway providing privileged access to the Supported Infrastructure by Service Provider personnel.
Service Provider Secure Service Delivery Network (SSDN)	A logical network environment which is hosted within the Service Provider's Service Management Centres (SMCs) which enables leveraged services to be operated and managed consistently and securely.
STRA	Security Threat & Risk Assessment Methodology attached as Appendix C, as changed through the Change Order Process.
Supported Infrastructure	All devices listed in Appendix C of the respective SOWs, the Servers and related equipment, firm and software that are subject to the Services being provided under the SOWs, the Operating System layer on all devices included in the foregoing, and the dedicated management tools agents used by the Service Provider in performing the Services, as the same may be changed from time to time over the Term pursuant to the Change Management Process or the Change Order Process, as applicable.
Virtual Image	Has the meaning given to it in the Virtual Server Services SOW.

Appendix A.1 – DSS Glossary

Note the following glossary and the terms and definitions set forth herein are applicable only to the PCI Data Security Services (PCI DSS) (Optional) described in Section 8.3 of this Statement of Work.

AAA	Authentication, authorization, and accounting protocol.
Accounting	Tracking of users' network resources.
Access control	Mechanisms that limit availability of information or information processing resources only to authorized persons or applications.
Account harvesting	Process of identifying existing user accounts based on trial and error. *[Note: Providing excessive information in error messages can disclose enough to make it easier for an attacker to penetrate and 'harvest' or compromise the system.]*
Account number	Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number (PAN).
Acquirer	Bankcard association member that initiates and maintains relationships with merchants that accept payment cards.
AES	Advanced encryption standard. Block cipher adopted by NIST in November 2001. Algorithm is specified in FIPS PUB 197.
ANSI	American National Standards Institute. Private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.
Anti-Virus Program	Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including viruses, worms, Trojan horses, spyware, and adware.
Application	Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications.
Approved Standards	Approved standards are standardized algorithms (like in ISO and ANSI) and well-known commercially available standards (like Blowfish) that meet the intent of strong cryptography. Examples of approved standards are AES (128 bits and higher), TDES (two or three independent keys), RSA (1024 bits) and ElGamal (1024 bits).

Asset	Information or information processing resources of an organization.
Audit Log	Chronological record of system activities. Provides a trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results. Sometimes specifically referred to as security audit trail.
Authentication	Process of verifying identity of a subject or process.
Authorization	Granting of access or other rights to a user, program, or process.
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss.
Cardholder	Customer to whom a card is issued or individual authorized to use the card.
Cardholder data	S. 15 plus any of the following:
	S15
Cardholder data environment	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.
Card Validation Value or Code	Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: • **CAV** Card Authentication Value (JCB payment cards) • **CVC** Card Validation Code (MasterCard payment cards)

• **CVV** Card Verification Value (Visa and Discover payment cards)

• **CSC** Card Security Code (American Express)

Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:

• **CID** Card Identification Number (American Express and Discover payment cards)

• **CAV2** Card Authentication Value 2 (JCB payment cards)

• **CVC2** Card Validation Code 2 (MasterCard payment cards)

• **CVV2** Card Verification Value 2 (Visa payment cards)

Compensating controls

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

CIS

Center for Internet Security. Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.

Compromise

Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.

Console

Screen and keyboard which permits access and control of the server or mainframe computer in a networked environment.

Consumer

Individual purchasing goods, services, or both.

Cookies	String of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information.
Cryptography	Discipline of mathematics and computer science concerned with information security and related issues, particularly encryption and authentication and such applications as access control. In computer and network security, a tool for access control and information confidentiality.
Database	Structured format for organizing and maintaining easily retrieved information. Simple database examples are tables and spreadsheets.
Data Base Administrator (DBA)	Database Administrator. Individual responsible for managing and administering databases.
DBA (Doing Business As)	Doing business as. Compliance validation levels are based on transaction volume of a DBA or chain of stores (not of a corporation that owns several chains).
Default accounts	System login account predefined in a manufactured system to permit initial access when system is first put into service.
Default password	Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known.
DES	Data Encryption Standard (DES). Block cipher elected as the official Federal Information Processing Standard (FIPS) for the United States in 1976. Successor is the Advanced Encryption Standard (AES).
DMZ	Demilitarized zone. Network added between a private and a public network to provide additional layer of security.
DNS	Domain name system or domain name server. System that stores information associated with domain names in a distributed database on networks, such as the Internet.
DSS	Data Security Standard.
Dual Control	Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable

	transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. See also, "split knowledge".
ECC	Elliptic curve cryptography. Approach to public-key cryptography based on elliptic curves over finite fields.
Egress	Traffic exiting a network across a communications link and into the customer's network.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
FIPS	Federal Information Processing Standard.
Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprises with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.
FTP	File transfer protocol.
GPRS	General Packet Radio Service. Mobile data service available to users of GSM mobile phones. Recognized for efficient use of limited bandwidth. Particularly suited for sending and receiving small bursts of data, such as e-mail and web browsing.
GSM	Global System for Mobile Communications. Popular standard for mobile phones Ubiquity of GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world.
Host	Main computer hardware on which computer software is resident.
Hosting Provider	Offer various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server.

HTTP	Hypertext transfer protocol. Open-internet protocol to transfer or convey information on the World Wide Web.
ID	Identity.
IDS/IPS	Intrusion Detection System/ Intrusion Prevention System. Used to identify and alert on network or system intrusion attempts. Composed of sensors which generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected. An IPS takes the additional step of blocking the attempted intrusion.
IETF	Internet Engineering Task Force. Large open international community of network designers, operators, vendors, and researchers concerned with evolution of Internet architecture and smooth operation of Internet. Open to any interested individual.
Information Security	Protection of information to insure confidentiality, integrity, and availability.
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information
Ingress	Traffic entering the network from across a communications link and the customer's network.
Intrusion detection Systems	See IDS.
IP	Internet protocol. Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.
IP address	Numeric code that uniquely identifies a particular computer on the Internet.
IP Spoofing	Technique used by an intruder to gain unauthorized access to computers. Intruder sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.

IPSEC	Internet Protocol Security (IPSEC). Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the -network layer.
ISO	International Organization for Standardization. Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland that coordinates the system **ISO 8583** Established standard for communication between financial systems.
Key	In cryptography, a key is an algorithmic value applied to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
L2TP	Layer 2 tunneling protocol. Protocol used to support virtual private networks (VPNs).
LAN	Local area network. Computer network covering a small area, often a building or group of buildings.
LPAR	Logical partition. Section of a disk which is not one of the primary partitions. Defined in a data block pointed to by the extended partition.
MAC	Message authentication code.
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business.
Malware	Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent.
Monitoring	Use of system that constantly oversees a computer network including for slow or failing systems and that notifies the user in case of outages or other alarms.
MPLS	Multi protocol label switching.

NAT	Network address translation. Known as network masquerading or IPmasquerading. Change of an IP address used within one network to a different IP address known within another network.
Network	Two or more computers connected together to share resources.
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
Network Security Scan	Automated tool that remotely checks merchant or service provider systems for vulnerabilities. Non-intrusive test involves probing external-facing systems based on external-facing IP addresses and reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network.
NIST	National Institute of Standards and Technology. Non-regulatory federal agency within U.S. Commerce Department's Technology Administration. Mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life.
Non consumer users	Any individual, excluding consumer customers, that accesses systems, including but not limited to employees, administrators, and third parties.
NTP	Protocol for synchronizing the clocks of computer systems over packet switched, variable-latency data networks.
OWASP	Open Web Application Security Project (see http://www.owasp.org.)
Payment Cardholder Environment	That part of the network that possesses cardholder data or sensitive authentication data.
PAN	Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number.
Password	A string of characters that serve as an authenticator of the user.

Pad	Packet assembler/disassembler. Communication device that formats outgoing data and strips data out of incoming packets. In cryptography, the one-time PAD is an encryption algorithm with text combined with a random key or *"pad"* that is as long as the plaintext and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable.
PAT	Port address translation. Feature of a network address translation (NAT) device that translates transmission control protocol (TCP) or user datagram protocol (UDP) connections made to a host and port on an outside network to a host and port on an inside network.
Patch	Quick-repair job for piece of programming. During software product beta test or try-out period and after product formal release, problems are found. A patch is provided quickly to users.
PCI	Payment Card Industry.
Penetration	Successful act of bypassing security mechanisms and gaining access to computer system.
Penetration Test	Security-oriented probing of computer system or network to seek out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect identify vulnerabilities and suggest security improvements.
PIN	Personal identification number.
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
POS	Point of sale.
Procedure	Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.
Protocol	Agreed-upon method of communication used within networks. Specification that describes rules and procedures that computer products should follow to perform activities on a network.
Public Network	Network established and operated by a telecommunications provider or recognized private company, for specific purpose of

	providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify, and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS, and GSM.
PVV	IN verification value. Encoded in magnetic stripe of payment card.

S15

RFC	Request for comments.
Re-keying	Process of changing cryptographic keys to limit amount of data to be encrypted with the same key.
Risk Analysis	Process that systematically identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure. Risk assessment.
Router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames.
Sanitization	Process for deleting sensitive data from a file, device, or system; or for modifying data so that it is useless if accessed in an attack.
SANS	SysAdmin, Audit, Network, Security Institute (See www.sans.org).
Security Officer	Primary responsible person for security related affairs of an organization.

Security policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete and track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction.
Separation of duties	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.
Server	Computer that providers a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, authentication, DNS, mail, proxy, and NTP.
Service Code	Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.
Service Provider	Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.
SHA	Secure Hash Algorithm. A family or set of related cryptographic hash functions. SHA-1 is most commonly used function. Use of unique salt value in the hashing function reduces the chances of a hashed value collision.
SNMP	Simple Network Management Protocol. Supports monitoring of network attached devices for any conditions that warrant administrative attention.

Split knowledge	Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
SQL	Structured (English) Query Language. Computer language used to create, modify, and retrieve data from relational database management systems.
SQL injection	Form of attack on database-driven web site. An attacker executes unauthorized SQL commands by taking advantage of insecure code on system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
SSH	Secure shell. Protocol suite providing encryption for network services like remote login or remote file transfer.
SSID	Service set identifier. Name assigned to wireless WiFi or IEEE S15 network.
SSL	Secure sockets layer. Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel.
Strong Cryptography	General term to indicate cryptography that is extremely resilient to cryptanalysis. That is, given the cryptographic method (algorithm or protocol), the cryptographic key or protected data is not exposed. The strength relies on the cryptographic key used. Effective size of the key should meet the minimum key size of comparable strengths recommendations. S. 15

S. 15

System Components	Any network component, server, or application included in or connected to the cardholder data environment.
TACACS	Terminal access controller access control system. Remote authentication protocol.
Tamper-resistance	System that is difficult to modify or subvert, even for an assailant with physical access to the system.
TCP	Transmission control protocol.
TDES	Triple Data Encription Standard also known as 3DES. Block cipher formed from the DES cipher by using it three times.
TELNET	Telephone network protocol. Typically used to provide user-oriented command line login sessions between hosts on the internet. Program originally designed to emulate a single terminal attached to the other computer.
Threat	Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.
TLS	Transport layer security. Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Token	Device that performs dynamic authentication.
Transaction data	Data related to electronic payment.
Truncation	Practice of removing data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.
Two-factor authentication	Authentication that requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors.
UDP	User datagram protocol.

UserID	A character string used to uniquely identify each user of a system.
Virus	Program or string of code that can replicate itself and cause modification or destruction of software or data.
VPN	Virtual private network. Private network established over a public network.
Vulnerability	Weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.
Vulnerability Scan	Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network.
WEP	Wired equivalent privacy. Protocol to prevent accidental eavesdropping and intended to provide comparable confidentiality to traditional wired network. Does not provide adequate security against intentional eavesdropping (for example, cryptanalysis)
WPA	WiFi Protected Access (WPA and WPA2). Security protocol for wireless (WiFi) networks. Created in response to several serious weaknesses in the WEP protocol.
XSS	Cross-site scripting. Type of security vulnerability typically found in web applications. Can be used by an attacker to gain elevated privilege to sensitive page content, session cookies, and variety of other objects.

Appendix B– Reporting

Report		Additional Criteria and/or Information
Provide a report of all third party individual accesses to the Support Infrastructure		Report listing all sub-contractor UserIDs
Anti-Virus Portal Reports		
Anti-Virus Motive Rolling Trend Report		
Anti-Virus Root Cause Rolling Trend Report		
Anti-Virus Severity Rolling Trend Report		
Per Server Policy Compliance Management detailed report (initial scans)		Provided for initial Policy Compliance Management Scan of existing Province Assets
A set of Standard Reports depicting anti-virus status		
A set of Standard Reports depicting anti-virus status		
A set of Standard Reports depicting anti-virus status		
A set of Standard Reports depicting anti-virus status		
A set of Standard Reports depicting IPS status	S15	
A set of Standard Reports depicting Consolidating Logging status		Report indicating statics of consolidated logging system such as: number of systems reporting; total number of log entries; number of alerts generated; etc
Per Server Policy Compliance Management detailed report.		For new and transformed devices
Security Health Check Report		As required by methodology provided by the Province as described in the Security SOW
Security Incident Recommendations Report		For validated Security Incidents that have findings impacting the security of the Support Infrastructure
Security Incident Summary Report		For validated Security Incidents that have findings impacting the security of the Support Infrastructure
Security Investigation Recommendations Report		For Service Provider Investigations that have findings

Report	Frequency	Additional Criteria and/or Information
		impacting the security of the Support Infrastructure
Security Investigation Summary Report	S. 15	For Service Provider Investigations that have findings impacting the security of the Support Infrastructure

Appendix C - Security Threat & Risk Assessment Methodology

See the JSRFP – Due Diligence – OCIO Information Security Branch requirements – V2.0.rtf Document.

Pages 319 through 327 redacted for the following reasons:
- -
S15, S15

MANAGED MAINFRAME SERVICES

SOW 4

TABLE OF CONTENTS

1. SOW 4 - SUMMARY AND SCOPE OF SERVICES

1.1 *Definitions*

Capitalized words used in this Statement of Work ("SOW") shall incorporate the meanings given to such words in the Master Services Agreement. In the event that a term is not defined in the Master Services Agreement, it shall have the meaning provided in Appendix A of this SOW or in the body of this SOW.

1.2 *Purpose of this Document*

1.2.1 General

The purpose of this SOW is to describe the scope and functions of the Managed Mainframe Services to be performed by Service Provider for the Province under the terms of the Agreement. This SOW sets forth the background and a general overview of the Managed Mainframe Services in Section 1.3 (*Managed Mainframe Services – Overview*) below, and describes such services in greater detail in this SOW below using an outcomes-based approach.

The outcomes-based approach used to describe the services in Section 2 (*Mainframe Services*), and Section 3 (*Optional Mainframe Services*) of this SOW is intended to allow Service Provider the ability to determine the most efficient manner of providing the Services so described while achieving all applicable SLAs or SLOs applicable to such Services; provided that in providing the Managed Mainframe Services the Service Provider complies, at all times, with the Privacy Obligations, the requirements of the Security SOW and the Province's Policies, as applicable.

Accordingly, the specific procedures, processes and associated tasks, required to be undertaken by Service Provider to perform the Managed Mainframe Services are not described in this SOW, but will be described more fully in the Managed Mainframe Operating Manual (defined below). As a result, it is the intention of the Parties that Service Provider will do what is required to deliver the Managed Mainframe Services in compliance with the requirements of this SOW, even though the specific procedures, processes and tasks to do so are not specifically identified or otherwise articulated in this SOW; provided that in doing so the Service Provider shall not be responsible for (or otherwise be required to undertake) those matters that are specified in this SOW as being the responsibility of the Province, a Client or a third party (where the third party is not a Subcontractor of Service Provider for purposes of providing Services under the Agreement).

1.2.2 Use RASIC Charts

Section 2 (*Mainframe Services*) and Section 3 (*Optional Mainframe Services*) of this SOW include "RASIC" charts that describe the responsibilities of the Province and Service Provider in respect of the Managed Mainframe Services. The "RASIC" charts are populated with "RASIC" indicators that are to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

P: means the Province

SP: means the Service Provider

1.2.3 Managed Mainframe Operating Manual

For greater clarification, it is the intention of the Parties that the specific procedures, processes, tasks and functions not described in this SOW that are required to be performed by Service Provider in order to deliver the Managed Mainframe Services shall be described in detail in the operating manual (the "**Managed Mainframe Operating Manual**"), to be prepared by Service Provider as part of the transformation activities under the Transformation SOW. The Managed Mainframe Operating Manual shall form part of the Manual described in Section 4.8 of the Agreement.

The Parties acknowledge that on the Hand-Over Date, the Managed Mainframe Operating Manual shall consist of the processes, procedures (and associated tasks and functions) that are in use by the Province immediately prior to the Hand-Over Date (the "**Province Procedures**") until the Province Procedures have been revised by Service Provider as contemplated in the Transformation SOW. The Parties acknowledge that the Province Procedures are in various states of completion and drafting, and will not necessarily articulate all processes, procedures, tasks and functions that will be required for Service Provider to provide the Managed Mainframe Services immediately following the Hand-Over Date.

1.2.4 Existing Service Locations, Transformation and Ownership

The Province outsourced the performance of mainframe services to a third party (the "**Current MF Provider**"). The term of the Current MF Agreement expires on January 31, 2011. Upon the expiration of the Current MF Agreement (the "**Managed Mainframe Services Commencement Date**"), the Service Provider shall be responsible for performing the Managed Mainframe Services described in this SOW. The terms and conditions regarding the migration of the responsibility for the mainframe services from the Current MF Provider to the Service Provider and the standing up of a new mainframe are set forth in the Transformation SOW.

As of the Managed Mainframe Services Commencement Date, the hardware and software that comprises the Mainframe System under this SOW and all additions and upgrades thereto shall at all times be and continued to be owned by the Service Provider unless and until such Mainframe System is transferred to the Province in accordance with Article 28 (*Default and Termination*) of the Agreement.

1.2.5 Appendices

The following Appendices are attached to and form part of this SOW, whether or not they are specifically referred to in this SOW:

Appendix A – Mainframe Services Definitions

Appendix B – Managed Mainframe Services Reports

Appendix C – Mainframe Hardware List

Appendix D - Mainframe System Software

Appendix E – Authorizations

1.3 *Managed Mainframe Services - Overview*

Managed Mainframe Services is the provision of a stable, secure mainframe computing platform and application production environment based on the Mainframe Hardware listed in Appendix C and Mainframe System Software listed in Appendix D, attached to this SOW (the "**Mainframe System**"). The Service Provider will provide fully managed Mainframe Services (described below) in a shared computing platform with very high levels of availability, reliability and security for large, shared computing workloads of a mission-critical nature. The Mainframe System is dedicated exclusively for the use of the Province and is shared among the Clients and such other third parties as directed by the Province, in writing. For greater certainty, the Service Provider shall use the Mainframe System for the purposes of providing the Managed Mainframe Services to the Province, Clients and such other third parties as directed by the Province.

This SOW describes, in detail, the scope and functions of the Managed Mainframe Services, provided by the Service Provider to the Province including, without limitation, hosting and storage management services in support of IBM mainframe platforms. Standard services, management tools and operational processes, and experienced staff enable the provision of a high quality and high availability Managed Mainframe Services.

The components of the Managed Mainframe Services are set forth below:

- Mainframe Services
    - Mainframe System Hardware Services
    - Mainframe System Software Services
    - Mainframe Storage Management Services
    - Mainframe Capacity Planning and Management Services
    - Performance Management Services
    - Mainframe Systems Operations
    - Batch Processing Services
    - Mainframe Client Technical Support Services
    - Mainframe Reporting Support Services
    - Mainframe Forms and Print Support Services
- Optional Mainframe Services
    - Extended Database Management Services
        - Extended Database Administration Services
        - Extended Database Consulting Services
        - Extended Database Production Support Services

1.4 *Related SOWs*

The Parties acknowledge and agree that this SOW is subject to the provisions of the Agreement and Schedules to the Agreement, however, the Parties have identified the following SOWs or Schedules to the Agreement as being important to the understanding of Managed Mainframe Services set forth in this SOW:

- Transformation SOW
- Services Management SOW
- Security SOW
- Data Centre SOW
- Business Continuity and Disaster Recovery Schedule

2. MAINFRAME SERVICES

The Mainframe Services comprise monitoring, maintaining and managing the Mainframe Hardware and Mainframe System Software configurations, including acquisition, installation, configuration, management, testing support and disposal of all Mainframe Hardware (including, for greater certainty, processor components) and Mainframe System Software.

2.1 *Mainframe System Hardware Services*

2.1.1 Mainframe System Hardware Environment Services

Mainframe System Hardware Environment Services is the integration (acquisition, installation, configuration, management, testing support, break/fix technical support and disposal) of the component hardware comprising the Mainframe Hardware. The Service Provider will provide Mainframe System Hardware Environment Services for the Mainframe System including, without limitation, the Mainframe Hardware components, personnel and support services to maintain a stable mainframe system environment that meets the requirements of the Province. The Service Provider will assemble Supplier Certified hardware components and integrate and test such Supplier Certified hardware components, to confirm that the hardware is functionally compatible when integrated together, prior to the installation into the Mainframe Hardware for production processing in the Mainframe System. The Mainframe Hardware listed in Appendix C, is a draft list of the Mainframe Hardware that the Parties anticipate may be required at the time the Service Provider assumes responsibility for the Managed Mainframe Services (not later than January 31, 2011), which Appendix C shall be updated by the Parties as contemplated in the Transformation SOW. Upon the completion of the updated list of Mainframe Hardware by the Parties, the attached Appendix C will be replaced and superseded by such updated Appendix C.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe System Hardware Environment Services	Responsibility	
Tasks and Functions	P	SP
Maintain and update the Mainframe Hardware Plan, on a monthly basis, which shall include, among other things, the Province's resource requirements as set forth in Section 2.4 (*Mainframe Capacity Planning and Management*) of this SOW		R
Prior to the introduction of any new Mainframe Hardware components into the Mainframe System, proactively research all implications of such new Mainframe Hardware to confirm that there is no adverse impact on the Mainframe System performance		R
Schedule and implement the Mainframe Hardware component upgrades as set forth in the Mainframe Hardware Plan and in accordance with Change Management Process		R
Manage all Mainframe Hardware component configuration and installation, including, without limitation, assembling Supplier Certified hardware components, integrating and testing such Supplier Certified hardware components for interoperability		R
Analyze and resolve all Mainframe Hardware component compatibility issues		R
Confirm all Mainframe Hardware components of the Mainframe System are in good working order and have appropriate vendor service agreements throughout the Term		R
Perform Mainframe Hardware installation and testing during the Change Window for the Mainframe System, as set forth in the Services Management SOW		R
Coordinate Client readiness in support of scheduled Mainframe Hardware installation and testing during the Change Window (for example, coordinating Client readiness for testing of Applications post Service Provider Change Window activity)	R	
Execute back-out procedures (fall back effort) set forth in the Services Management SOW, in accordance with the Change Management Process, to return the former Mainframe Hardware component configuration in the event of any problems that occur during any Mainframe Hardware component installation		R

Mainframe System Hardware Environment Services	Responsibility	
Tasks and Functions	P	SP
Plan and coordinate Mainframe Hardware component de-installations and disposal for all unused Mainframe Hardware components in accordance with the Mainframe Hardware Plan and the applicable Province Policy		R
Maintain Mainframe Hardware component configuration documentation (in electronic format) including, without limitation, all network component connections to the Mainframe System, for the Province's use		R
Provide Client briefings to the Managed Mainframe Services Client forums, monthly or otherwise upon the reasonable request of the Province, for new technologies, including planned technologies for implementation (including refresh of Mainframe Hardware) as well as updates on relevant technology options for future consideration		R

2.1.2 Mainframe Hardware Preventive Maintenance Services

Mainframe Hardware Preventive Maintenance Services is a service that provides for a stable Mainframe System through the application of regularly scheduled Mainframe Hardware component maintenance in accordance with Supplier recommendations.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Hardware Preventive Maintenance Services	Responsibility	
Tasks and Functions	P	SP
Prior to installation of preventive maintenance on the production Mainframe Hardware, test (wherever possible), analyze and resolve any compatibility issues with the hardware component Supplier's recommended preventive maintenance		R
Schedule Mainframe Hardware component preventive maintenance in accordance with Change Management Process		R
Provide documentation on any changes in Mainframe Hardware functions that may impact Application support when Supplier recommended preventive maintenance is applied in preparation for the change and to test the change in the Mainframe System Change Window, as contemplated in the Services Management SOW		R
Coordinate Client readiness in support of scheduled Mainframe System Change Window as contemplated in the Services Management SOW to allow for the installation and testing of Supplier recommended preventive maintenance (for	R	

Mainframe Hardware Preventive Maintenance Services	Responsibility	
Tasks and Functions	P	SP
example, coordinating Client readiness for testing of Applications post Service Provider Change Window activity)		
Implement Mainframe Hardware component preventive maintenance in accordance with Change Management Process		R
Execute back-out procedures, in accordance with the Change Management Process, to return to the former Mainframe Hardware component configuration in the event of any problems that occur during any Supplier recommended preventive maintenance installation		R

2.1.3 Mainframe Hardware Refresh Services

Mainframe Hardware Refresh Services are the continual replacement of hardware components comprising the Mainframe System, throughout the Term of the Agreement. Mainframe Hardware Refresh Services occur in accordance with the Mainframe Hardware Plan, unless the Parties agree otherwise to accelerate or delay any such Mainframe Hardware Refresh Services.

All Mainframe Hardware (excluding Swing Hardware), then current, will be listed in the Mainframe Hardware Plan, at the commencement of the Mainframe Services.

The major Mainframe Hardware Refresh activities during the Agreement Term are:

S15

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Hardware Refresh Services	Responsibility	
Tasks and Functions	P	SP
All Mainframe Hardware Refresh Services as contemplated in the Mainframe Hardware Plan will be carried out in accordance with the responsibilities and tasks set forth in Section 2.1.1 (*Mainframe System Hardware Environment Services*) of this SOW		R

Mainframe Hardware Refresh Services	Responsibility	
Tasks and Functions	P	SP
Update Mainframe Hardware component configuration documentation (in electronic format) after any Mainframe Hardware Refresh Services activities		R
Review the Mainframe Hardware components annually against the Mainframe Hardware Plan and determine whether any changes to the Mainframe Hardware Plan are necessary and make recommendations to the Province		R

2.2 *Mainframe System Software Services*

2.2.1 Mainframe System Software Environment Services

Mainframe System Software Environment Services is the integration (acquisition, installation, configuration, management, testing support, break/fix technical support and disposal) of the component software comprising the Mainframe System Software as required by the Province for development and operation of the Applications. For greater certainty, this includes the Interactive System Software Support Services sections for Mainframe CICS Support Services, Mainframe DB2 Support Services, Mainframe IMS Support Services and Mainframe MQSeries Support Services.

The Mainframe System Software is comprised of Standard Software and Non- Standard Software as more particularly described in Appendix D (*Mainframe System Software*).
In addition to the services described in this SOW, the Service Provider will carry out Mainframe System Software Environment Services in accordance with the Service Provider's Global Mainframe Software Distribution process. This distribution process centralizes the acquisition, integration and packaging of mainframe software products to achieve increased software implementation quality. The Parties acknowledge and agree that to the extent possible, industry standard software solutions will be preferred over proprietary software solutions with respect to the Mainframe System Software solution.

The Province is responsible for all aspects of the Applications. For greater certainty, services provided by the Service Provider under this section are limited to the Mainframe System Software and does not include Applications support.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe System Software Environment Services	Responsibility	
Tasks and Functions	P	SP
Maintain and update the Mainframe System Software Plan, on a monthly basis		R
Provide to the Province, on a monthly basis, a copy of the updated Mainframe System Software Plan		R

Mainframe System Software Environment Services Tasks and Functions	Responsibility P	 SP
Prior to the introduction of any Mainframe System Software components into the Mainframe System, proactively research implications of such new Mainframe System Software to confirm that there is no adverse impact on the Mainframe System performance		R
Schedule and implement the Mainframe System Software component upgrades as set forth in the Mainframe System Software Plan and in accordance with Change Management Process		R
Manage all Mainframe System Software component configuration and installation, including, without limitation, assembling Supplier Certified software components, integrating and testing such Supplier Certified software components for interoperability		R
The Service Provider will adopt configurations and parameters that allow Application-level interoperability with non-mainframe platforms (for example, other computer systems such as midrange or workstations), in areas where clear detailed industry standards are lacking		R
Analyze and resolve all Mainframe System Software component compatibility issues		R
Provide Mainframe System Software support including, but not limited to installation, stabilization and break/fix technical support		R
Based upon the Mainframe System Software Plan and any requirements for the Applications, provide the Service Provider with the requirements for any customization of the Mainframe System Software to address any special requirements for the Applications	R	
Customize the Mainframe System Software (including the Supplier provided software parameters) based upon the Province's requirements for the Applications (see row above)		R
Maintain Mainframe System Software product version and release levels, in accordance with the Mainframe System Software Plan, to maintain software integrity, software/hardware compatibility, and the availability of Applications and Mainframe Services		R
Upon the Province's request, track the utilization of Mainframe System Software on a Client by Client basis and report such utilization to the Province		R

Mainframe System Software Environment Services Tasks and Functions	Responsibility P	 SP
Identify Mainframe System Software (Non-Standard Software and Standard Software), if any, to be considered by the Province for replacement or retirement		R
Provide the Province with an alternate software solution where any component of the Mainframe System Software is identified for replacement and update Mainframe System Software Plan		R
Prepare Clients to transition off of Mainframe System Software being considered for retirement or replacement with an alternate software solution	R	
Where Non-Standard Software is being retired, track the utilization of such Non-Standard Software during the period until complete retirement and report such utilization to the Province upon the Province's request		R
Provide to the Province, on the third Friday of each month, a copy of the Mainframe System Software List as identified in Appendix D		R
In support of Service Provider Mainframe System Software installation the Province will verify Applications compatibility with the updated Mainframe System Software	R	
Carry out Mainframe System Software installation during the agreed Change Window, in accordance with the Change Management Process		R
Provide all Supplier management (including Supplier relationship management, Supplier negotiations and any Supplier contract amendments for Province approval) in connection with all Province licensed Non-Standard Software		R
Approve any and all amendments to the Province licensed Non-Standard Software agreements (including maintenance and support agreements for such Province licensed Non-Standard Software)	R	
On an annual basis provide the Province (in electronic format) current and updated pricing schedules for Non-Standard Software including, but not limited to, major upgrades not covered in the license agreement for such Non-Standard Software.		R
Inform the Province of any software Supplier notices and provide a copy of all Technical Information Bulletins (TIB) for the Non-Standard Software and the Standard Software		R

Mainframe System Software Environment Services	Responsibility	
Tasks and Functions	P	SP
Provide the Province with advance notice, as may be reasonable in the circumstances, of software Supplier license expiration or CPU serial number changes and take preventative measures in order that "license expiration" messages are not displayed to Clients (subject to the Province payment of fees directly to Suppliers for Non-Standard Software where such payment remains a Province responsibility)		R
Support, monitor for currency and update the Province's customized S. 15 S. 15		R
Provide software support, on a commercially reasonable efforts basis, for any and all Client licensed software that is hosted on the Mainframe System		R
On an ongoing basis, research other software products that may be of interest to or benefit the Province in connection with the Mainframe Services		R
Service Provider will liaise with the Province in connection with any and all Province licensed Non-Standard software requirements, during normal working hours		R

2.2.2 Mainframe System Software Preventive Maintenance Services

Mainframe System Software Preventive Maintenance Services is a schedule of planned maintenance and break/fix support to prevent software failures. The primary goal is to proactively carry out software maintenance to reduce the risk of Mainframe System failure before it actually occurs. In addition to services described in this SOW, the Service Provider will carry out Mainframe System Software Preventive Maintenance Services in accordance with the Service Provider's Global Mainframe Software Distribution process. This distribution process centralizes the acquisition, integration and packaging of mainframe software products to achieve increased software implementation quality.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe System Software Preventive Maintenance Services	Responsibility	
Tasks and Functions	P	SP
Implement Mainframe System Software Preventive Maintenance Services in accordance with the Mainframe System Software Plan and otherwise in the event of an incident		R

Mainframe System Software Preventive Maintenance Services	Responsibility	
Tasks and Functions	P	SP
Review Mainframe System Software maintenance information provided by the software Supplier, on an ongoing basis, to identify potential software issues relating to the Mainframe System		R
Where potential issues (see row above) are identified with the Mainframe System Software, apply preventive maintenance to Mainframe System Software products, as may be appropriate in the circumstances and in accordance with the Change Management Process set forth in Services Management SOW		R
Apply emergency fixes in accordance with the Change Management Process set forth in Services Management SOW		R
Prior to implementing any Mainframe System Software Preventive Maintenance Services to the Mainframe System Software, and any software component thereof, inform the Province of such material change and identify impacts to the Province or the Clients as a result of such material change For the purposes of this Section 2.2.2 (*Mainframe System Software Preventive Maintenance Services*), "material change" means a software change that involves product function changes that impact the Province or Clients and, in which case, the Service Provider will prepare and circulate a Technical Information Bulletin (TIB), in accordance with the Change Management Process		R
Approve all material changes to the Mainframe System Software, and any software component thereof, as a result of software maintenance, prior to the Service Provider implementing such material change	R	
Test the software preventive maintenance and research and resolve software compatibility issues before such software preventive maintenance is released for production processing		R
Design back-out processes to restore the former Mainframe System Software environment if unforeseen problems occur when carrying out the software preventive maintenance		R
Schedule down time in the Change Window, as appropriate, to perform required software preventive maintenance installation, in accordance with the Change Management Process		R

Mainframe System Software Preventive Maintenance Services	Responsibility	
Tasks and Functions	P	SP
Approve scheduled down time (within the Change Window and in emergencies), for software preventive maintenance, in accordance with the Change Management Process	R	
Coordinate Client readiness in support of scheduled Mainframe System down time to allow for the installation and testing of the required Mainframe System Software preventive maintenance (i.e., coordinating Client readiness for testing of Applications post Service Provider Change Window activity)	R	
Optimize Supplier provided parameters (tuning of the Supplier provided software product) for all Mainframe System Software in support of any preventive maintenance		R
Maintain Mainframe System Software product version and release levels, in accordance with the Mainframe System Software Plan, to sustain software integrity, software/hardware compatibility, and the availability of the Applications and Mainframe System Software Preventive Maintenance Services		R

2.2.3 Mainframe Software Refresh Services

Software Refresh Services is the planned replacement or upgrade of the Mainframe System Software components to maintain the currency of such Mainframe System Software, as more particularly described below and in accordance with the Mainframe System Software Plan.

In addition to maintaining the currency of the Mainframe System Software, the Service Provider will provide that the Mainframe System Software products continue to receive uninterrupted software Supplier support and maintenance throughout the Term of the Agreement.

The Service Provider will maintain the Mainframe System Software at the current version of the software available from the software Supplier ("N") or the next-to-current version of the software available from the software Supplier ("N-1") software release levels within 12 months of such software release becoming commercially available. Notwithstanding the foregoing, the Service Provider will, upon the request of the Province, maintain certain Mainframe System Software components at software release levels that are greater than N-1. In which case, the Service Provider will:

- provide that, at all times, all components of the Mainframe System Software will continue to receive uninterrupted software Supplier support and maintenance;
- use a phased process to implement Mainframe System Software changes, such that the changes will be applied first to the development, test and education of the Mainframe System and promptly thereafter to the production of the Mainframe System; and

- advise the Province of any and all software Supplier announcements to terminate support for any Mainframe System Software product and provide recommendations for dealing with such Supplier announcements.

Software Refresh Services	Responsibility	
Tasks and Functions	P	SP
Implement Mainframe System Software Refresh Services in accordance with the Mainframe System Software Plan that consists of the planned distribution and installation of the Integrated Software Refresh Package		R
Prior to implementing any Integrated Software Refresh Package or the Software Refresh Services to the Mainframe System Software, and any software component thereof, inform the Province		R
Approve all Integrated Software Refresh Packages, in accordance with the Change Management Process, prior to the Service Provider implementing such Integrated Software Refresh Packages	R	
Test the Integrated Software Refresh Packages and research and resolve any software compatibility issues before such refreshed software is released for production processing		R
Design back-out processes to restore to former Mainframe System Software environment if unforeseen problems occur when implementing the Integrated Software Refresh Packages		R
Approve scheduled down time within the Change Window, for the Integrated Software Refresh Packages, in accordance with the Change Management Process	R	
Coordinate Client readiness in support of scheduled Mainframe System down time to allow for the installation and testing of the required Integrated Software Refresh Packages (for example, coordinating Client readiness for testing of Applications post Service Provider Change Window activity)	R	
Optimize Supplier provided parameters (tuning of the Supplier provided software product) for all Mainframe System Software in support of any software refresh		R

Software Refresh Services	Responsibility	
Tasks and Functions	P	SP
Inform the Province of any software Supplier notices (including any impact statements and software Supplier refresh documentation) relating to the Integrated Software Refresh Packages, and prepare and circulate all technical information bulletins (TIB) relating thereto		R
Provide a limited refresh software test environment to allow the Province to test Application functions (for example, test Application functions in a development LPAR or region) in connection with any Integrated Software Refresh Package		R

2.2.4 Interactive System Software Support Services

Interactive System Software Support Services consist of the overall management of the following components of the Mainframe System Software: (a) database software; and (b) transaction processing software, that organizes the storage of Application data. For greater clarity, the database software and transaction processing software that organizes the storage of data is known as a database management system ("DBMS"). The Interactive System Software Support Services comprises the following (which are more fully described below):

- Mainframe DB2 Support Services
- Mainframe MQSeries Support Services
- Mainframe CICS Support Services
- Mainframe IMS Support Services
- Mainframe Service Request System (SRS) Services

2.2.4.1 *Mainframe DB2 Support Services*

Mainframe DB2 Support Services consists of all services required to Maintain and Support the Mainframe System DB2 Regions. For greater clarity, the services of an Applications database administrator or Applications backup and recovery are not included in this Section 2.2.4.1 as those services are Optional Services under Section 3 (Optional Mainframe Services) of this SOW.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe DB2 Support Services	Responsibility	
Tasks and Functions	P	SP
Maintain and Support the DB2 Regions		R
Analyze and tune the DB2 Regions to maintain or improve the overall DB2 Region performance		R
Perform backup and recovery services for each DB2 Region including DB2 system files (for greater clarity this includes but is not limited to the DB2 Region catalog and DB2 Region directory)		R
Start and stop DB2 Regions in accordance with Province requirements		R
Maintain and Support DB2 Region catalog and DB2 Region directory		R
If the Service Provider restores a DB2 Region, for any reason, perform synchronization of the Applications following the restore	R	
Upon any DB2 software upgrades, all Applications using DB2 Connect software to communicate to the DB2 Region on the Mainframe System, rebind the DB2 software to the DB2 Connect software such that Application can continue to access the DB2 Region on the Mainframe System		R

2.2.4.2 *Mainframe MQSeries Support Services*

Mainframe MQSeries Support Services consists of all services required to Maintain and Support the Mainframe System MQSeries Regions.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe MQSeries Support Services	Responsibility	
Tasks and Functions	P	SP
Maintain and Support the MQSeries Regions		R
Analyze and tune the MQSeries Regions to maintain or improve the overall MQSeries Region performance		R
Perform backup and recovery services for each MQSeries Region including MQSeries system files (for greater clarity this includes but is not limited to the MQSeries Region queues and MQSeries Region channels)		R
Start and stop MQSeries Regions in accordance with Province requirements		R

Mainframe MQSeries Support Services Tasks and Functions	Responsibility P	 SP
Create, manage, support and monitor MQSeries Region channels and MQSeries Region queues		R
Perform weekly cleanup of the development and test MQSeries Region dead letter queue		R
If the Service Provider restores a MQSeries Region, for any reason, perform synchronization of the Applications following the restore	R	
Maintain and Support all MQSeries bridges to IMS Regions and to CICS Regions		R

2.2.4.3 *Mainframe CICS Support Services*

Mainframe CICS Support Services consists of all services required to Maintain and Support the Mainframe System CICS Regions.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe CICS Support Services Tasks and Functions	Responsibility P	 SP
Maintain and Support the CICS Regions		R
Analyze and tune the CICS Regions to maintain or improve the overall CICS Region performance		R
Perform backup and recovery services for each CICS Region including CICS system files (for greater clarity this includes but is not limited to the CICS control files)		R
Start and stop CICS Regions in accordance with Province requirements		R
If the Service Provider restores a CICS Region, for any reason, perform synchronization of the Applications following the restore	R	
Maintain and Support the ImagePlus software workstation configuration within the appropriate CICS control files		R

2.2.4.4 *Mainframe IMS Support Services*

Mainframe IMS Support Services consists of all services required to Maintain and Support the Mainframe System IMS Regions. For greater clarity, the support under this section includes both IMS Database Manager (IMS/DB), IMS Transaction Manager (IMS/TM) and IMS Connect.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe IMS Support Services	Responsibility	
Tasks and Functions	P	SP
Maintain and Support the IMS Regions		R
Analyze and tune the IMS Regions to maintain or improve the overall IMS Region performance		R
Perform backup and recovery services for each IMS Region including IMS system files S. 15 S. 15		R
Start and stop IMS Regions in accordance with Province requirements		R
If the Service Provider restores a IMS Region, for any reason, perform synchronization of the Applications following the restore	R	
Maintain and Support IMS Database Manager (IMS/DB), IMS Transaction Manager (IMS/TM) and IMS Connect.		R

2.2.4.5 *Mainframe Service Request System (SRS) Services*

Mainframe Service Request System (SRS) Services comprises the Service Provider's maintenance and support of the Mainframe Service Request System (SRS) Services Application and the provision of software support to match developments in the following Mainframe System Software components: DB2, IMS, CICS and Security Server, for the Province to meet Province requirements.

The Mainframe Service Request System (SRS) Services Application is an application developed by the Province to provide a mechanism to enter Application change requests for the migration of IMS Regions, DB2 Regions and CICS Regions Application components.

All Applications that use the following Mainframe System Software components: DB2, IMS, CICS and Security Server, are included in the scope of the Mainframe Service Request System (SRS) Services.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Service Request System (SRS) Services	Responsibility	
Tasks and Functions	P	SP
Maintain and Support the Mainframe Service Request System (SRS) Services Application and the provision of software support to match developments in the following Mainframe System Software components: DB2, IMS, CICS and Security Server, for the Province to meet Province requirements		R
Provide administration management and execution of Mainframe Service Request System (SRS) Services Application requests submitted by the Province		R
Create and initiate Mainframe Service Request System (SRS) Services Application change requests using the guidelines and processes defined in the SRS User Guide	R	
Implement Mainframe Service Request System (SRS) Services Application requests (standard requests and emergency requests) as documented in the SRS User Guide		R
Provide assistance to Clients using the Mainframe Service Request System (SRS) Services Application, as may be required		R
Maintain and update the SRS User Guide to reflect any changes in the Mainframe Service Request System (SRS) Services Application, DB2, IMS, CICS and Security Server (including defining and documenting the operational procedures for the Applications' promotion controlled by the Mainframe Service Request System (SRS) Services Application)		R
Approve the operational procedures for the Applications' promotion controlled by the Mainframe Service Request System (SRS) Services Application	R	
Upon any Mainframe System Software upgrade, validate the Mainframe Service Request System (SRS) Services Application functionality and address any issues with functionality		R
During the annual Disaster Recovery Test, validate the Mainframe Service Request System (SRS) Services Application functionality and address any issues with functionality		R

2.2.5 Mainframe System Network Software Support Services

Mainframe System Network Software Support Services consists of those services required to maintain and support the Mainframe System Network Software to enable Mainframe System connectivity internally within the Mainframe System and through the Service Provider Data Centres to external networks (SPAN/BC and other external networks).

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe System Network Software Support Services Tasks and Functions	Responsibility	
	P	SP
Configure the Mainframe System Network Software to enable connectivity: • between the Mainframe System and the Service Provider's internal network for Managed Mainframe Services located within the Service Provider Data Centre in order to facilitate the connectivity between the Mainframe System and the SPAN/BC network or such other external networks as may be applicable; and • within the Mainframe System (for example, the connectivity between LPARs) This includes, without limitation, defining the nodes, terminals, printers and configuration files and such other services as required to enable such connectivity described above		R
Support the S15 utility (or such network interface) that provides the network logon menu interface to the Mainframe System		R
Maintain and Support the Mainframe System Network Software and configurations (for example, VTAM, TCP/IP and DRS) in accordance with Province Policy (in particular any IT Security Policies)		R
Maintain and Support any modifications to the Mainframe System Network Software (exits and usermods)		R
Test all Mainframe System Network Software components in conjunction with Mainframe System Software maintenance and upgrades		R

2.2.6 Mainframe System Software Backup and Restore Services

Mainframe System Software Backup and Restore Services is the creation of copies of the Mainframe System Software that will be used to perform Mainframe System-level recovery in the event Mainframe System data is not accessible in the STMS Calgary Data Centre. This

service is limited to on-site restoration and does not include any off-site, disaster recovery capabilities.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe System Software Backup and Restore Services	Responsibility	
Tasks and Functions	P	SP
Implement an appropriate backup schedule for Mainframe System Software to provide that Mainframe System files and user catalogues are available in the event of a Mainframe System failure		R
Perform regular full volume backups of Mainframe System Software and data on the Mainframe System in order to recover from isolated device failure, or to recover the processing platform in the case of a Disaster (incremental backups include non-database user volumes and are generally available for clients to recover snapshots of individual datasets)		R
Maintain and update Mainframe System back-up processes documentation (in electronic format)		R
Adjust Mainframe System back-up processes as Mainframe System requirements change		R
Inform the Province of any changes to timing, sequencing, content, tools, or any other aspects that may be related to or affecting Mainframe System backup and restore of the Applications		R
Consult with Clients concerning any changes to timing, sequencing, content, tools, or any other aspects that may be related to or affecting Mainframe System backup and restoration of the Applications and notify the Service Provider of issues identified, as applicable	R	
Should a recovery of the Mainframe System Software be required, recover the Mainframe System Software in the STMS Calgary Data Centre and promptly notify the Province in accordance with the Services Management SOW (Incident Management Process)		R
Synchronize the Application backups with Mainframe System Software backups	R	

2.3 *Mainframe Storage Management Services*

2.3.1 Mainframe Storage Services

Mainframe Storage Services is the management of the storage of Data on the Mainframe System. The Service Provider will provide automated Data storage management within the Mainframe System to enable all Data to be managed at the dataset level and to select the correct data storage Media. Within the Mainframe System managed storage environment there are both online and removable storage media, commonly referred to as disk, virtual tape, and tape.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Storage Services	Responsibility	
Tasks and Functions	P	SP
In the event of a change in the Province's Data requirements (or any one of the Data availability, accessibility, performance, and retention requirements), the Province will notify the Service Provider		R
Assess changes in the Province's Data requirements		R
Assist the Province in determining the level of required service that will maximize data performance and minimize storage costs having regard for the Province's new Data requirements		R
Notify the Province, in writing, of the impact on the Mainframe System storage and make recommendations as to how the Province's Data requirements may be met (the implementation of such new Data requirements will be processed through the Change Management Process)		R
Amend the Mainframe System storage policies and processes to meet the new Province requirements, if applicable		R
Update the Automation Routines based upon the amended Mainframe System Storage policies and processes to meet the new Province requirements, if applicable		R
Verify the integrity of storage media catalogues (tape and disk) by auditing discrepancies between the VTOC and the Storage Media Catalogue and notify the Client who is the primary owner of the dataset		R

Mainframe Storage Services Tasks and Functions	Responsibility P	 SP
Provide all Media management services (hardware support and maintenance, Media support and maintenance, tape library administration, including, without limitation, tape vaulting, control procedures and analysis, initialize tapes, return tapes to scratch status) to provide continual Data accessibility and Media reliability		R
Provide a sufficient number of blank Media and "scratch" tapes to respond to removable-media system mount requests and respond in a timely way to such requests		R
Monitor and maintain Mainframe System storage performance in accordance with Section 2.5 (*Performance Management Services*) of this SOW		R
Audit tape Media inventory (comparing physical tapes against catalogue) on an annual basis or more frequently, upon the request of the Province, and promptly report results of such audit to the Province and highlight discrepancies		R
Support and maintain the IBM Aggregate Backup And Recovery Support (ABARS) software tool		R

2.3.2 Client Removable Media Support Services

Client Removable Media Support Services is the handling by the Service Provider of removable Media (typically tape) that is: (a) created at the Service Provider Data Centres; or (b) shipped to the Service Provider Data Centres or received by the Service Provider from an Approved Client, or such other Person as approved by the Parties.

Upon the creation or receipt of the Media, as contemplated by this Section, the Service Provider will catalogue, store, prepare for processing, and then prepare for return by the Service Provider to the Approved Client, or such other Person as approved by the Parties, for pick up. The Service Provider will only be responsible for all Media while such Media is in the custody or control of the Service Provider.

The Parties acknowledge and agree that the Client Removable Media Support Services described below will be replaced with Secure FTP Services, with the intention that this will occur prior to January 2011. Notwithstanding that the Province is moving to Secure FTP Services, the Media handling services described in this Section will continue to be supported by the Service Provider, as necessary.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Client Removable Media Support Services Tasks and Functions	Responsibility P	 SP
Notify the Province, on an ongoing basis, of the type of Media that is supported in connection with the Client Removable Media Support Services (for example, moving from IBM 3590A/SUN 9490 to SUN 9840D)		R
Receive, track, and prepare removable Media		R
Log all Media shipments received by the Service Provider and maintain current the Media inventory and supporting documentation that documents the receipt, location and status of the Media (for example, the destruction of the Media, in accordance with Province Policy and the return of the Media to the Approved Client, or such other Person approved by the Parties)		R
Based on instructions from an Approved Client, or such other Person approved by the Parties, locate, package and prepare the removable Media for pick up by the Approved Client, or such other Person approved by the Parties (or their respective representatives)		R
Log all Media shipments sent from the Service Provider Data Centres, attach the proper records to allow correct delivery and permit tracing. Confirm the receipt of the Media was received by the Approved Client, or such other Person approved by the Parties		R
Retain all Media shipment logs in accordance with the provisions of the Agreement and provide a summary of such Media logs to the Province, on a quarterly basis		R
Provide special Media shipment instructions to the Service Provider, if applicable, regarding how to ship removable Media to the Province or Approved Client, or such other Person approved by the Parties or any specified location	R	
Provide that any Media shipments out of the Service Provider Data Centres, that are requested by Province or an Approved Client, or such other Person approved by the Parties		R
Pay all shipping charges related to the shipment of removable Media, as contemplated in this Section, to or from the Province, an Approved Client, or such other Person approved by the Parties	R	

2.3.3 Secure FTP Services

File Transfer Protocol (FTP) is the protocol for exchanging files over the Internet. FTP works by electronically transferring/moving files from one server to another server. The functions of the secure version of FTP, commonly referred to as Secure FTP, is defined in the Security SOW.

2.3.4 Off-Site Data Storage Disaster Recovery Services

Off-Site Data Storage Disaster Recovery Services is the management of removable Media and/or electronically transmittable recovery data created in the form of a copy of such data at the Disaster Recovery Site. The Service Provider will transfer all recovery data from a VTE located at the Service Provider Data Centre where the production Mainframe System is located to the VTE at the Disaster Recovery Site, in the event of a Disaster to recover the operating environment of the Mainframe System for the Province at the Disaster Recovery Site. All Media on the VTE located at the Service Provider Data Centre where the production Mainframe System is located and at the Disaster Recovery Site will be encrypted.

By using an online VTE vaulting solution, the data for recovery is written directly to the disaster recovery site (the Disaster Recovery Site) so that the recovery data will be available at the time of a Disaster declaration or test.

As part of the Off-Site Data Storage Disaster Recovery Services, archive data (the Province's long term retention records) may be written to this site for long term retention, eliminating their need to be stored at the primary processing site.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Off-Site Data Storage Disaster Recovery Services	Responsibility	
Tasks and Functions	P	SP
Ensure that all data is encrypted prior to its transfer from the Service Provider Data Centre where the production Mainframe System is located to the Disaster Recovery Site		R
Manage the electronic transfer (or transport) of the data to and from the Disaster Recovery Site (including, for greater certainty, the transfer of data from a Disaster Recovery Site to a different Disaster Recovery Site as agreed by the Parties)		R
Support Province electronic recall of data from the Disaster Recovery Site		R
In the event of a Disaster, create an online vault facility plan to convert the Disaster Recovery Site into a production mainframe system environment and to secure another off-site secure location as the new Disaster recovery site in substitution for the Disaster Recovery Site (for greater clarity, this approach will be implemented by the Service Provider in the event that a return to the original		R

Off-Site Data Storage Disaster Recovery Services Tasks and Functions	Responsibility P	 SP
location of the production Mainframe System is not possible as a result of the Disaster)		
Maintain the online vault solution to ensure that data can be electronically transferred to the Disaster Recovery Site (or such other designated recovery center as the Parties mutually agree in writing), including without limitation, maintaining data mirroring between the VTE at the Service Provider Data Centre where the production Mainframe System is located and the VTE at the Disaster Recovery Site		R
Backup Applications (including data within such Applications) to ensure backup rotation and frequency are adequate for Applications recovery	R	

2.3.5 Hardware Tape Encryption Services

Hardware Tape Encryption Services is the encryption of data at the tape drive or tape drive controller level, so that the encryption processing has been off-loaded from the main processor, the Mainframe System. Within the first six months after the commencement of the Mainframe Services under this SOW, the Service Provider will provide the Hardware Tape Encryption Services and the default for all data on tapes is that the data on the tapes will be encrypted through the tape hardware. Notwithstanding the tape encryption default, the Province may request (in writing) that certain data not be encrypted, at the Province's option.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Hardware Tape Encryption Services Tasks and Functions	Responsibility P	 SP
Copy existing non-encrypted tape data to encrypted tape media within the first six months after commencing the Mainframe Services under this SOW		R
In the event of media errors such that the data cannot be copied, the Service Provider will notify the Province promptly		R
In the event of any Media errors that result in the data not being capable of being read or processed, the Service Provider will notify the Province promptly		R
Acquire the Mainframe Hardware encryption key(s)		R

Hardware Tape Encryption Services Tasks and Functions	Responsibility P	 SP
Securely dispose of old encryption key(s) and the Media in the event of a tape drive refresh that changes the encryption process (the destruction of the Media, in accordance with Province Policy)		R
The Mainframe Hardware encryption keys will be stored with the encrypting tape drives at the Service Provider Data Centre and at the Disaster Recovery Site		R
At the request of the Province, rather than encrypting tape data using the Mainframe Hardware, the Service Provider will provide the software encryption of tape Media as part of the Client Removable Media Support Services		R

2.4 *Mainframe Capacity Planning and Management Services*

Mainframe Capacity Planning and Management Services is the process of analyzing the current and future Mainframe System Resource Capacity requirements of the Province. This process uses the Province's forecasted workload as well as planned and potential service and technology changes for the Service Provider to make recommendations to provide that:

- sufficient Mainframe System Resource Capacity is available to meet the Province's expected future business requirements; and
- Mainframe System Resources are effectively utilized to optimize the Mainframe System Resource Capacity.

In the event the Parties determine, through the Mainframe Capacity Planning and Management process, that changes to the Mainframe System Resources are required, then such changes will be addressed through the Change Management Process, in accordance with the Services Management SOW.

The Service Provider shall provide the Province with Mainframe Capacity Planning and Management Services, which consists of monitoring the Mainframe System Resources for capacity utilization (providing for the availability of MIPS cycles for Mainframe System processing, Mainframe System storage for Clients as needed and Mainframe System memory, as needed), forecasting of aggregate Mainframe System Resource Capacity requirements of the Province (MIPS, memory and storage usage, based upon historical data provided by the Service Provider (for the 24 month period immediately preceding such forecast), and updated by the Province), and analyzing and reporting of Mainframe System Resources trends (for example, MIPS, memory and storage usage).

The Service Provider will deliver to the Province:

- the Capacity Plan, on a semi annual basis, (between the periods January – March and July – September once the Service Provider receives the Province's forecasted information (see below)), which plan will set forth the forecasted aggregate

Mainframe System Resource Capacity requirements of the Province for the next 24 month period; and

- the Capacity Report, on a monthly basis, which report will set forth the actual usage of Mainframe System Resources for the immediately preceding month against forecasted Mainframe System Resources for such month. The Capacity Report will be delivered by the Service Provider to the Province no later than fifteen (15) calendar days following the end of the actual month being reported.

The Province will provide to the Service Provider, on a semi annual basis (between the periods January – March and July – September), the Province's forecasted Mainframe System Resources capacity requirements for the next 24 month period, including the following:

- Processor capacity (MIPS)
- Storage capacity (gigabytes)

In addition to the Mainframe System Resources capacity requirements above, where possible, the Province will define and provide to the Service Provider the following to support the Mainframe Capacity Planning and Management process:

- new Applications to be implemented on the Mainframe System;
- growth or decline in the then current Applications on the Mainframe System; and
- Application retirement plans and implications for the Mainframe Systems.

Upon receipt of the Province's forecasted Mainframe System Resource Capacity requirements and potential changes to the Applications as described above, the Service Provider will review the Province's forecasted capacity requirements and update the Service Provider's two-year Mainframe System Capacity Plan for the Mainframe System Resources requirements (processor capacity (MIPS) and storage capacity (gigabytes)). In updating the Capacity Plan, the Service Provider will take into consideration technology changes, service changes and actual resource capacity utilization and will provide the updated Capacity Plan to the Province for review and comments.

The Service Provider will identify to the Province any significant deviations in trends, concerns or anomalies found in the actual base configuration resource usage and provide analysis and supporting data to identify the system and/or client areas/components contributing to the growth in order that appropriate decisions can be made by the Parties.

The Mainframe Capacity Planning and Management Services will be performed in accordance with the LSPR MIPS Rating, for the term of the Agreement, unless amended through the Change Order Process.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Capacity Planning and Management Services Tasks and Functions	P	SP
Within five days after commencing the Managed Mainframe Services, provide a duly amended Mainframe Hardware List in the form attached as Appendix C to this SOW from which the Parties may measure Resource Capacity over time		R
Monitor Mainframe System Resource utilization on a daily basis		R
Report the Mainframe System Resource Capacity utilization to the Province on a monthly basis (see Appendix B – Managed Mainframe Services Reports)		R
Perform Mainframe System Resource Capacity trend analysis at the aggregate level and for each of the Major Resource Categories at a discrete level (for example, including without limitation, IMS and CICS) to determine whether such Mainframe System Resource utilization is trending upward or trending downward		R
Report Client changes in Mainframe System Resource Capacity usage (on a Client by Client basis) as part of the resource capacity trend analysis, to the Province on a monthly basis (see Appendix B – Managed Mainframe Services Reports)		R
Perform Mainframe System Resource Capacity modeling for Major Resource Categories, which modeling will include setting forth possible future outcomes for Mainframe System Resource Capacity utilization to achieve the optimal Mainframe System Resource utilization (for example, modeling scenarios related to significant configuration, system or workload changes to determine the utilization implications)		R
On a semi-annual basis, between the periods January – March and July – September, with such specific dates in each year as mutually agreed by the Parties, provide the Province with capacity forecast templates populated with each Client's historical Mainframe System Resource usage data (for the previous 24 month period) which data will be used by the Clients to forecast Mainframe System Resource capacity usage requirements for the next 24 month period		R
Within approximately 30 days after receiving the forecast templates populated with each Client's historical Mainframe System Resource usage data, the Province will provide the Service Provider with the Province's forecasted Mainframe System Resource Capacity requirements based on each Client's usage projections documented in the forecast templates	R	

Mainframe Capacity Planning and Management Services Tasks and Functions	P	SP
Analyze Application workload and the forecasted Client Mainframe System Resource usage data, based upon the completed templates above, and determine whether changes are required to the Mainframe Hardware or the Mainframe System Software		R
Advise the Province of the LSPR MIPS Rating: • annually; • when there is a Mainframe Hardware configuration change, or • when the Service Provider is notified that LSPR MIPS Rating has been changed		R
Advise the Province of any expected Mainframe System Resource capacity impacts or benefits that may arise due to Mainframe Hardware or Mainframe System Software maintenance or new technology becoming available		R

2.5 *Performance Management Services*

Performance Management Services consist of defining, collecting, monitoring, measuring, analyzing and trending Mainframe System performance information to proactively identify anomalies in the Mainframe System, avoid potential performance problems and issues with the Mainframe System, as well as support any incident resolution, as required. The Mainframe System performance information monitored will include, but is not limited to, processor activity, memory usage, data storage devices and network devices such as controllers and channels. Performance changes will be implemented to modify the configuration and tune the Mainframe System to optimize the effectiveness and efficiency of the Mainframe System platform environment in accordance with the Change Management processes set forth in the Services Management SOW.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Performance Management Services Tasks and Functions	Responsibility P	 SP
Monitor, analyze, tune and report on Mainframe System Resources per Appendix B - *Managed Mainframe Services Reports*)		R
Perform Application tuning and performance monitoring to optimize Mainframe System Resource consumption	R	

Performance Management Services Tasks and Functions	Responsibility P	 SP
Provide support to the Province for Applications tuning to optimize Mainframe System Resource consumption		R
Provide recommendations to the Province on techniques to enhance the performance of the Applications running on the Mainframe System and the impact on the Province's Application performance		R
Monitor and maintain Mainframe System Software configuration to manage Mainframe System performance and workload throughput		R
Proactively monitor and manage Mainframe System Resource allocations within the Mainframe System and implement changes to the Mainframe System Resource allocation to resolve Mainframe System performance issues, as may be appropriate		R
Proactively identify and resolve any and all Mainframe System Resource performance problems		R
Notify, where possible, the Service Provider of any known material changes to Province Mainframe System workload with an appropriate lead time, if application or related scheduled changes could impact system performance	R	
In the event of degraded Mainframe Services, promptly provide details to the Province regarding any and all impacts to the Mainframe System Clients		R

2.6 *Mainframe Systems Operations*

2.6.1 System Availability Management Services

System Availability Management Services consists of monitoring all Mainframe System components so that they remain operational and capable of processing Mainframe System workloads, and provides any support required for the delivery of a stable, functional system environment that meets all availability service levels.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

System Availability Management Services Tasks and Functions	Responsibility P	 SP
Perform Mainframe System operation functions and system console operations		R
Monitor the Mainframe System controls and take the necessary actions based on detected alerts		R
Perform Mainframe System operational system failure recovery functions as needed		R
Notify the Service Provider regarding the Province's activities that will impact the Service Provider during the Province's scheduled Change Window	R	

2.6.2 Mainframe System Console Operations Services

Mainframe System Console Operations Services is the physical monitoring of the overall health of the Mainframe System and responding, as appropriate, to the following:

- Exception Events; and
- ordinary course scheduled actions (for example, starting and stopping systems resources such as CICS Regions, IMS transactions, batch initiators, network connections and the operating systems).

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe System Console Operations Services Tasks and Functions	Responsibility P	 SP
Provide 24/7 Basis monitoring, using Service Provider staff resources, of the Mainframe System console and resolve Exception Events		R
Performing scheduled Mainframe System tasks that are not otherwise addressed through the Mainframe Automated Operations		R
Maintain and update Mainframe System operational support documentation for all internal procedures and services (in electronic format)		R

2.6.3 Mainframe Automated Operations

Mainframe Automated Operations is the automation and management of the Mainframe System and the Exception Events that occur on the Mainframe System using software tools, processes and support team resources. The Service Provider shall provide the Mainframe Automated

Operations to the Province using the Service Provider's automation tools (software tools that will reside on the Mainframe System and some software tools that will reside on dedicated servers, such Service Provider tools are listed in the attached Appendix D) and support team resources. Examples of Mainframe Automated Operations shall include, without limitation, the following:

- executing controlled Mainframe System shutdown;
- controlled Mainframe System start-up (IPL, Initial Program Load); and
- monitoring a wide range of Mainframe System tasks.

The Service Provider will use the Service Provider's automation tools to design and maintain Mainframe System automation processes. As the Managed Mainframe Services (including, for greater certainty, Mainframe Hardware and Mainframe System Software) evolve over time, the Service Provider will continually update the Mainframe Automated Operations to address new requirements.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Automated Operations	Responsibility	
Tasks and Functions	P	SP
Design and implement a comprehensive Mainframe Automated Operations strategy that: • minimizes errors and outages; and • incorporates the Service Provider's (and its Affiliates') experience and knowledge base, as such experience and knowledge base evolves over the Term and adapts to changes in the Managed Mainframe Services		R
Create, maintain, and execute Mainframe System start-up and Mainframe System shutdown scripts (scripts are a set of instructions to start-up and shutdown the Mainframe System)		R
Design and implement, as required, automated replacement processes for manual processes for the Mainframe System		R
Design and implement reactive automation processes to address Exception Events and to respond appropriately to system alerts and Exception Event notifications (for example, an alert is created if a batch job terminates for any reason before it is supposed to, or if a batch job does not complete by a specific time)		R
Design and implement proactive automation processes which assist in preventing Exception Events on the Mainframe System (for example, automated monitoring of disk storage pools and alerting the system operators if a threshold is exceeded)		R

Mainframe Automated Operations	Responsibility	
Tasks and Functions	P	SP
Promptly notify the Province of all Exception Events that adversely affects any one or more Clients and provide the Province with the options (in writing if requested) that may be taken to resolve such Exception Event		R
Upon receipt of notification of an Exception Event from the Service Provider, the Province will advise the Service Provider of the option that the Service Provider is required to implement to resolve the Exception Event	R	
Advise Province of any significant trends or recurring Exception Events arising out of the Mainframe Automated Operations that may impact the Managed Mainframe Services or require Client notification		R

2.7 *Batch Processing Services*

Batch Processing Services consists of all activities associated with running batch processing jobs on the Mainframe System including, without limitation, administering the automated scheduling system to support a batch-processing environment. Batch process job submission is managed through:

(a) the automated scheduling software product ("Automated Scheduling System") which is provided, managed and monitored by the Service Provider and is a fully managed batch job administration and monitoring service by the Service Provider ("Fully Managed Batch Processing"); or

(b) the Automated Scheduling System in which the Province submits the batch job directly to the Automated Scheduling System and the Province manages and monitors the batch jobs and the Service Provider also monitors the batch jobs ("Partially Managed Batch Processing"); or

(c) manual batch processing jobs, submitted outside of the Automated Scheduling System, in which the Province submits the batch job directly to the JES2 queue and the Province manages the batch job administration (including manually submitting and monitoring the batch jobs) and the Service Provider monitors the batch jobs in accordance with the Mainframe System Console Operations Services ("Manual Batch Processing").

The Province may select either Fully Managed Batch Processing or Partially Managed Batch Processing or Manual Batch Processing, for the execution of its batch jobs, in its discretion. In the case of Fully Managed Batch Processing, Partially Managed Batch Processing and Manual Batch Processing, the Province (and each Client) can view and manage the schedule of batch processing jobs independent of other Clients. All changes, restarts, cancellations and similar actions, for one Client will not affect another Client or Clients.

The RASIC table below applies to the Mainframe Batch Monitoring Services for Fully Managed Batch Processing, Partially Managed Batch Processing and Manual Batch Processing, unless expressly indicated otherwise in the RASIC table.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Batch Processing Services	Responsibility	
Tasks and Functions	P	SP
Provide appropriate Mainframe System resources (for example, CPU, storage and supporting controllers and bandwidth) including operational resources, tools, and procedures to support the processing		R
Support "No Priority Batch" service which allows Clients to run non-deadline dependent jobs on the Mainframe System without incurring billable MIPS under the Province Mainframe System cost recovery process (a special account code is assigned to each Client that allows No Priority Batch jobs to be run without incurring charges for CPU use) for Manual Batch Processing		R
Utilize the Province's batch processing definitions for the delivery of Batch Processing Services		R
Maintain the tools and facilities for the Province to perform Partially Managed Batch Processing and Manual Batch Processing		R
Provide problem resolution and support for Batch Processing Services issues		R

2.7.1 Mainframe Batch Monitoring Services

Mainframe Batch Monitoring Services consists of all activities associated with monitoring the execution functions of an Application's batch processing, scheduled within the Automated Scheduling System. The objective of Mainframe System production batch monitoring is to have all pre-defined Application cycles execute in the proper sequence with the results (the batch job completion) produced within the defined processing time frames for completion associated with the batch scheduling activity.

The RASIC table below applies to the Mainframe Batch Monitoring Services for Fully Managed Batch Processing, Partially Managed Batch Processing and Manual Batch Processing, unless expressly indicated otherwise in the RASIC table.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Batch Monitoring Services Tasks and Functions	Responsibility P	 SP
Monitor the execution of scheduled batch cycles as per agreed scheduling requirements (for example, identifying and investigating late or overdue batch jobs) for Fully Managed Batch Processing and Partially Managed Batch Processing		R
Monitor the availability of the appropriate Mainframe System resources for timely batch job execution (where there Mainframe System resources are not sufficient for timely batch job execution, the Service Provider will report an incident in accordance with the provisions of the Services Management SOW)		R
Escalate abnormally terminated batch jobs to the Province (identifying the appropriate Applications team, where applicable) for Fully Managed Batch Processing and Partially Managed Batch Processing		R
Assist the Province in performing Problem identification and resolution consisting of production batch restarts and reruns for Fully Managed Batch Processing and Partially Managed Batch Processing		R
Provide and maintain the agreed notification list: • for the Applications batch cycle; and • Application escalation contacts • (the "Client Contact Lists")	R	
Provide the schedule for specific batch jobs that are to be repeated or run on an Application's batch cycle (for example, the schedule for a batch job that must be run on a daily, weekly, monthly basis) for the Fully Managed Batch Processing	R	

2.7.2 Mainframe Batch Scheduling Services

Mainframe Batch Scheduling Services consists of all activities associated with defining and maintaining an Application's batch processing within the Automated Scheduling System. The objective of Mainframe System production batch scheduling is to have all pre-defined Application cycles execute in the proper sequence with the results (the batch job completion) produced within the defined processing time frames for completion associated with the batch scheduling activity.

The Service Provider will be responsible for: (a) managing the batch job scheduling for workload monitored and controlled by the Service Provider as part of the Batch Processing Services; and (b) entering the scheduling requests of Clients for the workload of Clients who manage their own automated demand batch job schedules. For greater clarity, there is an Automated Scheduling System scheduler that is used by multiple Clients across LPARs.

The RASIC table below applies to the Mainframe Batch Monitoring Services for Fully Managed Batch Processing and Partially Managed Batch Processing, unless expressly indicated otherwise in the RASIC table.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Batch Scheduling Services	Responsibility	
Tasks and Functions	P	SP
Receive and review the Province's batch requirements for Fully Managed Batch Processing		R
Provide technical and operational support for the automated scheduler and tools		R
Add and maintain the defined Clients' batch job schedule into the Automated Scheduling System based on the Clients' batch requirements for Fully Managed Batch Processing		R
Maintain the database for the Automated Scheduling System		R
Resolve batch scheduling issues for Fully Managed Batch Processing and notify the Province of such scheduling issues and the issue resolution, through the Incident Management Process of the Services Management SOW		R
Provide assistance to Province to resolve any batch scheduling issues for the Partially Managed Batch Processing		R
Provide to the Service Provider, and maintain and update on an ongoing basis, a list of authorized Province personnel, in the form attached as Appendix E – Authorizations, who are authorized to modify batch schedule(s) (such Appendix E – Authorizations will be provided by the Province to the Service Provider prior to the date that the Service Provider commences the provision of the Managed Mainframe Services)	R	
Permit only authorized Province personnel, as identified in writing by the Province in the form of Appendix E – Authorizations, to modify batch schedule(s)		R
Provide batch schedule requirements, including job flow, dependencies, and directions for exception conditions (for example, batch job restart instructions and batch job callout (or escalation notification) instructions)	R	
Provide the Service Provider with changes to the Client Contact Lists	R	

Mainframe Batch Scheduling Services	Responsibility	
Tasks and Functions	P	SP
Maintain the Client Contact Lists for Client batch job schedules for batch job restart instructions and batch job callout (or escalation notification) instructions		R

2.8 *Mainframe Client Technical Support Services*

Mainframe Client Technical Support Services is the technical and operational support provided by the Service Provider to the Province (Mainframe System Clients) to facilitate efficient and effective use of the Managed Mainframe Services , and to respond to the Province (the Clients) requests for support or assistance related to the Managed Mainframe Services to achieve a high level of Client satisfaction.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Client Technical Support Services	Responsibility	
Tasks and Functions	P	SP
Monitor (during Prime Time) the Mainframe support contact email addresses, acknowledge receipt of all emails and provide a response, or an estimated time for a full response, within 7 business hours (measured via incident tickets raised by Clients)		R
Provide technical advice and support to Clients receiving Managed Mainframe Services and Applications developers during Hours of Service (for example, Mainframe System Software features, functions, new services, how to and such other features or functions)		R
Provide technical advice and recommendations as the Province and Clients reasonably request (for example, product research, project support, application tuning, interoperability and such other recommendations)		R
Provide technical and/or operations support staff to attend meetings with Clients, as required		R
Support Client forums and committees by making presentations on aspects of the Managed Mainframe Services: including, without limitation, monthly Mainframe Advisory / Database Administrator Forum (MAF/DBAF), quarterly Windows Working Group (WWG), Resource Usage Reporting Group, and such other forums and committees as reasonably appropriate		R

Mainframe Client Technical Support Services Tasks and Functions	Responsibility P	 SP
At least annually, the Service Provider will prepare and make presentation(s) to Client forums on the Mainframe Software Plans and Mainframe Hardware Plans for the Province's next year (April 1 to March 31)		R
Provide the Service Provider with the Managed Mainframe Services User Guide (MVS User Guide) and any supporting guides and documentation to be used in connection with the Mainframe System and the Managed Mainframe Services (for example, the SRS User Guide and such other guides as applicable (collectively, the "User Guides"))	R	
Maintain and update the User Guides for the Mainframe System and the Managed Mainframe Services (products and services targeted to Clients), in the format required by the Province on a continuous basis as appropriate		R
Provide a copy of all software supplier user guides and technical documentation for software comprising the Mainframe System Software ,via direct access to software supplier web sites if permitted or by providing an electronic version to the Province		R
The Service Provider will order software supplier documentation for delivery to the Province or Clients upon request (the Parties acknowledge that the costs incurred by the Service Provider to obtain such software supplier documentation will be reimbursed by the Province)		R

2.9 *Mainframe Reporting Support Services*

Mainframe Reporting Support Services is the Service Provider' responsibility for delivering the reports listed in Appendix B (*Managed Mainframe Services Reports*) (the "Mainframe Reports"), in the form and format, containing the content as identified by the Province and at the frequency as set forth in Appendix B (*Managed Mainframe Services Reports*). Mainframe Reporting Support Services includes the standard reports customarily delivered by the Service Provider to its customers in connection with mainframe services (such reports at the Effective Date are listed in Appendix B (*Managed Mainframe Services Reports*), as such customary reports may change over the Term of the Agreement). In addition, notwithstanding the provisions of Article 13 (*Reporting and Annual Operating Plan*) and Schedule 5 (*Special Terms*) of the Agreement, the Service Provider will provide the Province with ad hoc or on demand reporting, as reasonably requested by the Province.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Reporting Support Services Tasks and Functions	Responsibility P	 SP
Create, update, maintain and deliver the Mainframe Reports		R
Respond to reasonable requests for ad hoc or on demand reports as contemplated in the paragraph above and provide such reports		R
Capture and retain the full system raw SMF daily data on tape for seven years		R
Capture and retain the summarized SMF database on tape for ten years (the summarized data is a small subset of the raw SMF data to support the INFO Reporting System and other WTS specialized reporting requirements for accounting, chargeback, performance and capacity purposes. This summary data includes detail to understand workload and capacity changes by service and Client)		R
Detailed data to support Mainframe Systems Services reporting functions as set out in Appendix B will be retained in accordance with the Province's Operational Records Classification Systems (ORCS) and the Administrative Records Classification System (ARCS) policy		R
Provide high level report of major storage categories with metrics related to configuration diagram (see Appendix B (*Managed Mainframe Services Reports*) – Storage Utilization Report)		R
Provide high level mainframe network report on usage statistics and patterns S. 15 (see Appendix B (*Managed Mainframe Services Reports*) – Network Utilization Report)		R
Analyze, review, determine and apply new MIPS Accounting Factors to support associated MIPS reporting for capacity forecasting, utilization and the Province's WTS Mainframe System cost recovery process		R
Apply MIPS Accounting Factor changes to the SMS accounting records annually, on April 1st, in accordance with the Change Management Process		R
Report the attainment of Mainframe System reliability and timeliness targets for mainframe service components on a monthly basis (see Appendix B (*Managed Mainframe Services Reports*) – Service Measures Report). These service component targets are an addendum to the Mainframe System Service Levels and Key Measurements in Schedule 11-A and 11-B of the Agreement		R

2.10 *Mainframe Forms and Print Support Services*

Mainframe Forms and Print Support Services is the management and customization of the printing and presentation Mainframe System Software products used for printing and online document viewing from the Mainframe System. The provision of Client support for all print-related Mainframe System Software, custom code and utilities required to support routing output to mainframe network attached printers are within the scope of the Mainframe Forms and Print Support Services.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Mainframe Forms and Print Support Services	Responsibility	
Tasks and Functions	P	SP
Provide the Service Provider with the forms requirements	R	
Maintain and Support forms based on the forms requirements		R
Maintain and Support custom code including but not limited to the following S. 15		R
Provide administration and support for the ViewDirect Mainframe System Software product		R
As part of the annual Disaster Recovery Test, validate print to network attached printers		R
Execute Province requests for all printer stops and starts		R
Provide monthly reports to the Province detailing volumes by Clients and form type for Mainframe System print jobs (see Appendix B – Managed Mainframe Services Reports)		R
Provide support for new and existing print applications		R
Initiate service requests for changes to or of support of print definitions	R	
Receive and implement service requests		R

3. OPTIONAL MAINFRAME SERVICES

The following services are available to the Province as optional services and are subject to being requested by the Province through Service Request/Province Ordering System request (under the Services Management SOW) on a Standard Time & Materials basis.

3.1 *Extended Database Management Services*

Extended Database Management Services includes the following components: Extended Database Administration Services, Extended Database Consulting Services and Extended Database Production Support Services as defined below. Upon the request of the Province, the Service Provider will provide the Extended Database Management Services, or any component of the Extended Database Management Services.

3.1.1 Extended Database Administration Services

Extended Database Administration Services is the management of the physical Application databases. Extended Database Administration Services includes, without limitation, database monitoring, backups, reorganization and recovery of the physical Application database, as may be necessary. Extended Database Administration Services apply to the following Mainframe System Software products: IMS, DB2, VSAM, and ImagePlus.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Extended Database Administration Services	Responsibility	
Tasks and Functions	P	SP
Perform all tasks and functions required to create a backup copy of the Application database		R
Carry out all tasks and functions for the Application database recovery to restore an Application database from a backup copy and associated log files		R
Carry out Application database reorganization tasks and functions including, but not limited to, unloading the Application database, redefining the Application database file structure and reloading the Application database with the objective to improve the Application database file structure space usage and the associated Application performance		R
Monitor the Application database monitoring including, but not limited to, analyzing database physical metrics and usage activity with the objective to identify Application database performance improvements (for example, the need for an Application database reorganization for better utilization or Application performance)		R

Extended Database Administration Services Tasks and Functions	Responsibility	
	P	SP
Provide Application database administration disaster recovery in order to recover an Application database from a backup copy and associated log files during a Disaster Recovery Test or during a Disaster to the Disaster Recovery Site		R

3.1.2 Extended Database Consulting Services

Extended Database Consulting Services is the assistance to Application developers as may be necessary in connection with the design and development of an Application database. Extended Database Consulting Services apply to the following Mainframe System Software products: IMS, DB2, VSAM, and ImagePlus.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Extended Database Consulting Services Tasks and Functions	Responsibility	
	P	SP
Assist Application developers to define the Application requirements		R
Assist Application developers to choose an appropriate DBMS to meet the Application requirements		R
Assist the Application developers to create and improve Application code in connection with the Mainframe System		R
Assist the Application developers to create and improve Application code to provide the required Application database access to the DBMS (the Application view or schema)		R
Provide physical Application database design consulting services to define the Application database fields and the field characteristics, as required to meet the Application requirements		R
Provide logical Application database design consulting services to define the logical view or schema of the physical Application database so that only the required Application data is managed by an Application		R
Manage the control blocks for the IMS component of the Mainframe System Software including, without limitation, the process of defining, changing and removing the IMS database definitions (DBD), the associated program structure blocks (PSB) and message format services (MFS) to an IMS Region		R

Extended Database Consulting Services Tasks and Functions	Responsibility P	 SP
Maintain and Support of the IMS Region, DB2 Region, CICS Region (including the VSAM file structure for each of IMS Region, DB2 Region, CICS Region) and the ImagePlus Mainframe System Software product, for the development, testing, education and production regions		R
Assist the Province with assessing Application database utilities and tools and recommend utilities and tools to meet the Application requirements		R
Identify and recommend new or advanced Application database utilities to achieve cost-savings, with the implementation of any new or advanced Application database utilities being subject to the Province's approval in writing		R
Assist Application developers to identify Application database runtime performance issues		R
Assist Application developers to assess the need for changes (including upgrades) within the Application database		R

3.1.3 Extended Database Production Support Services

Extended Database Production Support Services is the management (administration, performance, tuning, reorganization, changes, and diagnostics) of the Application databases in the production environment of the Mainframe System. Extended Database Production Support Services apply to the following Mainframe System Software products: IMS, DB2, VSAM, and ImagePlus.

Service Provider and the Province will perform the tasks or functions as indicated in the RASIC chart below.

Extended Database Production Support Services Tasks and Functions	Responsibility P	 SP
Provide Application database management in a production environment including, but not limited to, Application database administration, Application database performance tuning, Application database implementation, Application database maintenance in accordance with the Application database standards and Application database technical support		R
Monitor Application database performance to ensure availability of application data to the Applications		R

Extended Database Production Support Services Tasks and Functions	Responsibility P	 SP
Identify and recommend to the Province modifications to the Application database to improve the Application performance		R
Perform Application database tuning and Application database reorganization as required to maintain Application performance requirements		R
Perform Application database diagnostics to assist in Problem resolution		R
Make changes to Application database size to improve the Application performance		R
Modify views or schemas and convert data from one view or schema to another to provide appropriate Application access		R
Make changes to tables, columns, indexes, synonyms, links, stored procedures, and other Application database objects to meet Application requirements		R
Plan for changes in the size of Application databases due to changing business requirements		R
Schedule and implementation of changes in the size of Application databases, such changes based on business information provided by the Province, with such implementation being subject to the Province's approval		R
Create the physical Application database in the DBMS including, without limitation, create indices and access methods		R
Provide emergency production support, on a 24/7 Basis, to resolve Application database incidents and problems		R
Recommend Application database maintenance cycles including, without limitation, Application database backups and Application database reorganizations		R
Accept or reject Application database maintenance cycle recommendations	R	
Implement approved Application database maintenance cycle recommendations		R

Extended Database Production Support Services Tasks and Functions	Responsibility P	 SP
Validate Mainframe System Software upgrades to DBMS or OS		R
Process access authorities to Application databases and assist with Client Application database security requests		R

4. Appendices

APPENDIX A - MAINFRAME SERVICES DEFINITIONS

Definable Term	Definition
24/7 Basis	means 24 hours per day, 7 days per week, 365 days per year.
Abend	(ABnormal END) A type of system error in which a task or program fails to execute properly (for example, "abnormally ends") and the term is also used as the name for a type of error message that indicates such a failure has occurred.
ACS Routines	means Automatic Class Selection and ACS routines are one of the mechanisms DFSMS/MVS provides to help automate storage management (using ACS routines provides centralized control of storage management and automatically associated SMS classes and groups with datasets).
Applications	means the business applications developed and maintained by the Province Clients.
Approved Client	means a Client that is listed on the attached Appendix E as such appendix may be updated over the Term of the Agreement.
Automated Scheduling System	has the meaning given to it in Section 2.7(a) of this SOW.
Automation Routines	means the set of instructions and threshold settings used to manage Mainframe System resources (for example, batch and online storage thresholds, alerts, print spool and disk pools).
Batch Processing Services	means the execution of a series of programs ("jobs") on a computer without human interaction (batch jobs are set up so they can be run to completion without human interaction, so all input data is preselected through scripts or command-line parameters as opposed to "online" or interactive programs which prompt the user for such input) as such services are more particularly described in Section 2.7 of this SOW.
Capacity Management	means the responsible for making sure that the Resource Capacity of Managed Mainframe Services and the Managed Mainframe Services infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all Resources required to deliver the Managed Mainframe Services, and plans for short, medium and long term business requirements of the Province.
Capacity Plan	means part of the report "Capacity Planning and Utilization Report – *Month/Year"* found in Appendix B (*Managed Mainframe Services Reports*).
Capacity Planning	means the activity within Capacity Management responsible for creating a Capacity Plan.

Definable Term	Definition
Capacity Report	Means part of the report" Capacity Planning and Utilization Report – *Month/Year"* found in Appendix B (*Managed Mainframe Services Reports*).
Central Processing Unit (CPU)	means a machine that can execute computer programs.
Change Management Process	means the change process described in the Services Management SOW.
Change Window	has the meaning given to such term in the Services Management SOW (the regularly scheduled time frame, from 6:00 AM to 9:00 AM (PST) weekly on Sunday where changes to the systems environment are tested and implemented).
CICS	means the Customer Information Control System, a transaction server that runs primarily on IBM mainframe systems under z/OS and is a transaction manager designed for rapid, high-volume online processing (this processing is mostly interactive (screen-oriented), but background transactions are possible and such software product is listed in Appendix D – Mainframe System Software as CICS Transaction Server).
CICS Region	means a collection of resources controlled by CICS as a unit (a CICS resource is any facility or component of a CICS system that is required to perform a task. The resources in a region include programs, Basic Mapping Support (BM) map sets, transactions, terminals, files, transient data queues, temporary storage queues, and journals. A CICS region consists of the following components: Resource definition databases, Libraries and Services and subsystems.
Client	has the meaning given to it in the Agreement and, for the purposes of this SOW, includes any and all Broader Public Sector entities purchasing Managed Mainframe Services directly from WTS.
Client Contact Lists	means the document given to the Service Provider by the Province that relates a Client to an Application for Batch Processing Services.
Client Removable Media Support Services	means the services described in Section 2.3.2 of this SOW.
CLIST	means the high-level interpretive language that enables end users to work more efficiently with TSO/E. Programs called CLISTs may be written to perform routine and complex programming tasks.TSO/E is part of the IBM zOS software.
Data	means the information collected, administered and managed by the Province in electronic form (or a printed version thereof), which may be accessed by a Service Provider, including, for greater certainty, backups and other copies of such Data.

Definable Term	Definition
Database Administration or DBA	means the function of managing and maintaining database management systems (DBMS) software (mainstream DBMS software such as IBM's DB2 and IMS require ongoing management and systems DBAs focus on the physical aspects of database administration such as DBMS installation, configuration, patching, upgrades, backups, restores, refreshes, performance optimization, maintenance and Disaster Recovery).
DB2	means one of IBM's families of relational database management system (RDBMS) (or, as IBM now calls it, data server) software products within IBM's broader Information Management Software line.
DB2 Region	means a Mainframe System subsystem, a secondary or subordinate system that is usually capable of operating independently of, or asynchronously with, a controlling system. A DB2 Region is a distinct instance of a relational DBMS. Its software controls the creation, organization, and modification of a database and access to the data that the database stores.
DBMS	has the meaning given to it in Section 2.2.4 of this SOW.
Disaster Recovery	means the restoration, at a location other than the STMS Calgary Data Centre, of the Managed Mainframe Services following a declared Disaster.
Disaster Recovery Plan (DRP)	means the plan prepared by the Service Provider to provide a full recovery of Managed Mainframe Services upon a declared Disaster or a Disaster Recovery Test.
Disaster Recovery Site	means the secured off-site storage location for Disaster Recovery purposes, which shall be SunGard Canada in Ontario or such other location as the Parties mutually agree in writing.
Disaster Recovery Test	also known as the "Information Technology Recovery Exercise (ITRE)", means the annual activity that exercises the Disaster Recovery Plan for the Managed Mainframe Services delivered by the Service Provider under the Agreement which exercise includes the recovery of the Mainframe System and a subset of Client Applications.
DRS (Dynamic Report System)	allows CICS online transactions, other TP monitor applications and batch programs to dynamically create reports on the JES spool or route to network attached printers.
Exception Event	means abnormal conditions such as job Abends, transaction Abends and system alerts such as performance threshold warnings, and includes, but is not limited to, starting and stopping systems resources such as CICS regions, IMS transactions, batch initiators, network connections and the operating systems.
Extended Database Administration Services	means the services described in Section 3.1.1 of this SOW.
Extended Database Consulting Services	means the services described in Section 3.1.2 of this SOW.

Definable Term	Definition
Extended Database Management Services	means the services described in Section 3.1 of this SOW.
Extended Database Production Support Services	means the services described in Section 3.1.3 of this SOW.
Fully Managed Batch Processing	has the meaning given to it in Section 2.7(a) of this SOW.
Global Mainframe Software Distribution	means the Service Provider process that centralizes the acquisition, integration and packaging of Mainframe System Software products to achieve increased software implementation quality.
Hardware Tape Encryption Services	means the services described in Section 2.3.5 of this SOW.
Hours of Operation	means 24 hours per day, 7 days per week ("24 x 7"), excluding Change Windows and Scheduled Outages
Hours of Service	means 7:00 a.m. to 5:00 p.m. (PST), Monday to Friday, excluding Holidays
ImagePlus	means the mainframe content management software product for document imaging and folder management.
IMS	means IBM's Information Management System (IMS) which is a joint hierarchical database and information management system with extensive transaction processing capabilities.
IMS Database Manager (IMS/DB)	means the database component of an IMS Region that supports the access to and storage of data in a database.
IMS Region	means a Mainframe System subsystem, a secondary or subordinate system that is usually capable of operating independently of, or asynchronously with, a controlling system. An IMS Region is a distinct instance of a DBMS. The IMS software enables terminal users, batch applications and database utilities to retrieve and modify the data within a database, ensures the retrieval is current and maintains system log information to allow data recovery.
IMS Transaction Manager (IMS/TM)	means a transaction manager (IMS TM, also known as IMS DC). A transaction manager interacts with an online user (connected through VTAM or TCP/IP, including 3270 and Web user interfaces) or another application to process Application data.
INFO Reporting System	means the "INFO Reports" found in Appendix B (*Managed Mainframe Services Reports*).
Integrated Software Refresh Package	means the set of software products that are acquired from the software Supplier(s) and then installed and tested on the Service Provider test system to verify the functionality of the software products as a single product offering.

Definable Term	Definition
Interactive System Software Support Services	means the services described in Section 2.2.4 of this SOW.
ISPF	means Interactive System Product Facility and is an IBM product that is part of the zOS Base in the software list (Appendix D).
JES2 (Job Entry Subsystem)	means the component of IBM's Multiple Virtual Storage (MVS) operating system that reads in jobs, interprets their Job Control Language (JCL) and schedules their execution.
LPAR	means the division of a single computer into two or more independent environments, each running its own operating system. An LPAR enables formerly separate systems to be consolidated on a single machine.
LSPR MIPS Rating	means the MIPS Large Systems Performance Reference rating system based on IBM benchmarks (IBM runs a series of benchmark's that are made publicly available, to determine the MIPS rating for the various processors).
Mainframe Automated Operations	means the services described in Section 2.6.3 of this SOW.
Mainframe Batch Monitoring Services	means the services described in Section 2.7.1 of this SOW.
Mainframe Batch Scheduling Services	means the services described in Section 2.7.2 of this SOW.
Mainframe CICS Support Services	means the services described in Section 2.2.4.3 of this SOW.
Mainframe Client Technical Support Services	means the services described in Section 2.7.3 of this SOW.
Mainframe DB2 Support Services	means the services described in Section 2.2.4.1 of this SOW.
Mainframe Forms and Print Support Services	means the services described in Section 2.10 of this SOW.
Mainframe Hardware	means the hardware components found in Appendix C (*Mainframe Hardware List*).
Mainframe Hardware Plan	means the report "Mainframe Hardware Plan" found in Appendix B (*Managed Mainframe Services Reports*).

Definable Term	Definition
Mainframe Hardware Preventive Maintenance Services	means the services described in Section 2.1.2 of this SOW.
Mainframe Hardware Refresh Services	means the services described in Section 2.1.3 of this SOW.
Mainframe IMS Support Services	means the services described in Section 2.2.4.4 of this SOW.
Mainframe MQSeries Support Services	means the services described in Section 2.2.4.2 of this SOW.
Mainframe Reporting Support Services	means the services described in Section 2.9 of this SOW.
Mainframe Reports	has the meaning given to it in Section 2.9 of this SOW.
Mainframe Service Request System (SRS) Services	means the services described in Section 2.2.4.5 of this SOW and is the application change facility for the migration of IMS and CICS components. The Service Request System is an ISPF menu-driven system.
Mainframe Services	means the services described in Section 2 of this SOW.
Mainframe Storage Management Services	means the services described in Section 2.3 of this SOW.
Mainframe Storage Services	means the services described in Section 2.3.1 of this SOW.
Mainframe System	has the meaning given to it in Section 1.3 of this SOW.
Mainframe System Console Operations Services	means the services described in Section 2.6.2 of this SOW.
Mainframe System Hardware Environment Services	means the services described in Section 2.1.1 of this SOW.
Mainframe System Network Software	means the network software components of the software products that are listed in this SOW at Appendix D (*Mainframe System Software*) and any associated documentation.

Definable Term	Definition
Mainframe System Network Software Support Services	means the services described in Section 2.2.5 of this SOW.
Mainframe System Software	means the software products that are listed in this SOW at Appendix D (*Mainframe System Software*) and any associated documentation.
Mainframe System Software Backup and Restore Services	means the services described in Section 2.2.6 of this SOW.
Mainframe System Software Environment Services	means the services described in Section 2.2.1 of this SOW.
Mainframe System Software Plan	means the report "Mainframe Systems Software Plan" found in Appendix B (*Managed Mainframe Services Reports*).
Mainframe System Software Preventive Maintenance Services	means the services described in Section 2.2.2 of this SOW.
Mainframe Systems Operations	means the services described in Section 2.6 of this SOW.
Maintain and Support	in connection with the Mainframe Hardware and Mainframe System Software includes, without limitation, configuration, acquisition, installation, configuration, management, testing support, break/fix support, end user support and disposal, as applicable, of such Mainframe Hardware and Mainframe System Software.
Major Resource Categories	Means MIPS, DASD, Tape, CPU seconds, workload volumes by service (for example, TSO, IMS, CICS, Batch, DB2).
Managed Mainframe Operating Manual	has the meaning given to it in Section 1.2.3 of this SOW.
Managed Mainframe Services	means the services described in this SOW.
Manual Batch Processing	has the meaning given to it in Section 2.7(c) of this SOW.
Media	means hardware that stores data (for example, DASD, tape).
MIPS (Millions of Instructions Per Second)	means an approximate measure of a computer's processor power.

Definable Term	Definition
MIPS Accounting Factors	means the capture ratios, billing factors, system factor, and processor ratings applied to accounting records to normalize processor usage across changes in operating systems levels and hardware technology. Factors will change from time to time subject to the mutual agreement of the Parties, as new operating systems, processors and Client workloads change (such review and adjustment by the Parties will be annually on April 1st).
MQSeries	means the software product that provides the communication path between applications that may be on different platforms.
MQSeries Region	means a Mainframe System subsystem, a secondary or subordinate system that is usually capable of operating independently of, or asynchronously with, a controlling system. An MQSeries is a queue manager that owns and manages the set of resources that include; page sets, logs, connections through which different application environments (CICS, IMS, and Batch) can access the MQSeries and a MQSeries channel initiator.
MVS	means IBM's mainframe operating system superseded by OS/390 and later z/OS.
N	has the meaning given to it in Section 2.2.3 of this SOW.
N-1	has the meaning given to it in Section 2.2.3 of this SOW.
NETSOL Interface	Network Solicitor logon menu to the Mainframe System.
Non-Standard Software	means the software products that the Service Provider or the Province is responsible for providing in connection with the Mainframe System, as listed in Appendix D.2.
No Priority Batch or NPB	means the service that allows customers to run large non-deadline dependent jobs without incurring billable MIPS under the Province Mainframe System cost recovery methodology (a special account code is assigned to each Client and allows NPB jobs to be run without incurring charges for CPU use, however, charges are still accumulated by the Province for I/O and print services).
Offsite Data Storage Disaster Recovery Services	means the services described in Section 2.3.4 of this SOW.
Operating System	means the main control program that runs a computer and sets the standard for running application programs. An operating system is responsible for functions such as memory allocation, managing programs and errors and directing input and output.
Partially Managed Batch Processing	has the meaning given to it in Section 2.7(b) of this SOW.
Performance Management Services	means the services described in Section 2.5 of this SOW.
Prime Time	means the hours from 8:00 a.m. to 5:00 p.m. (PST) Monday through Friday, excluding statutory holidays.

Definable Term	Definition
Resource	means any physical or virtual systems component of limited availability within a computer system. It includes Mainframe hardware and software computing resource components that are measured to support the Mainframe Services Capacity Planning and Management Services, Performance Management Services, and Managed Mainframe Services Reports (Appendix B). The Resource components include, but are not limited to, MIPS, memory, CPU time, disk, tape, started tasks, LPARs, regions and transactions (for example, CICS, IMS, DB2, DDF) and network throughput.
Resource Capacity	means the measure or extent to which the Resources are used against the available or target system capacity.
Resource Usage Reporting Group	Means a sub-committee of the Windows Working Group (WWG).
Scheduled Outage	means any time period negotiated through the Change Management Process under the Services Management SOW, where the Managed Mainframe Services (or any component of the Managed Mainframe Services) are not available to the Province (Clients), excluding Change Windows.
Secure FTP Services	means the services described in Section 2.3.3 of this SOW.
Security Server	means the IBM security software product that provides access control and auditing functionality for the Mainframe System. Security Server is also known as Resource Access Control Facility (RACF).
SMF	means the IBM System Management Facility and is a component of the Operating System that provides a standardized method for recording system activities. These records include, but are not limited to: I/O; network activity; software usage; error conditions; and processor utilization.
Software Refresh Services	means the services described in Section 2.2.3 of this SOW.
SPAN/BC	known as the Shared Provincial Access Network for British Columbia (SPAN/BC), means the shared private network that enables connectivity and electronic service delivery between the B.C. government, the broader public sector, the business community and citizens of the province.
SRS User Guide	means the end user documentation of how to use the Service Request System (SRS).
Standard Software	means the software products provided by the Service Provider and listed in Appendix D.1.
STMS Calgary Data Centre	has the meaning given to it in the Data Centre SOW.
Storage Media Catalogue	means the combination of master and user catalogs that are used to manage all of the mainframe files.
SunGard	means the subcontractor of the Disaster Recovery Site.

Definable Term	Definition
Supplier Certified	has two meanings. The first means that the Service Provider has tested the hardware components that comprise the Mainframe Hardware to provide that such hardware is functionally compatible when integrated together. The second means that the Service Provider has tested the software components that comprise the Mainframe System Software to provide that such software is functionally compatible when integrated together.
Swing Hardware	means temporary hardware for transition of the Province's Managed Mainframe Services from its existing service provider as of the Effective Date to the Service Provider.
System Availability Management Services	means the services described in Section 2.6.1 of this SOW.
TCP/IP	means the Internet Protocol Suite: A combination of the Transmission Control Protocol and the Internet Protocol.
TSO	means the Time Sharing Option and is an interactive time-sharing environment for the lineage of IBM mainframe operating systems. "Time-sharing" means that many persons can access MVS concurrently.
User Guides	has the meaning given to it in Section 2.8 of this SOW.
ViewDirect	means the software product listed in Appendix D.
VSAM	means the Virtual Storage Access Method and is one of IBM's access methods for direct-access files.
VTAM	means Virtual Telecommunications Access Method and is the main Systems Network Architecture (SNA) subsystem resident in an IBM mainframe that manages session establishment and data flow between terminals and application programs, or between application programs.
VTE	means Virtual Tape Environment that is intermediate DASD with associated tape control units and tape drives.
Volume Table Of Contents (VTOC)	means the disk storage volume table of contents (which is the table of contents listing the Data on the disk).
Windows Working Group (WWG)	means the Windows Working Group Client forum lead by WTS that supports the usage forecasting of Managed Mainframe Services (MIPS, Storage) for both the capacity planning process and the allocation and recovery of Mainframe costs by the Province from the Clients of the Managed Mainframe Services.

APPENDIX B – MANAGED MAINFRAME SERVICES REPORTS

All Report Names referenced in the following table will be provided by the Service Provider to the Province.

Report Name	Description	Link to SOW Section	Frequency	# of Reports (approx.)	Format Hardcopy or Softcopy
Capacity Planning and Utilization Report – *"Month/Year"*	Capacity utilization synopsis and recommendations, including: • Analysis of 11th Hour Usage, Prime Shift Usage, and Actual vs. Forecast; • A recommendation re MVS Processor, DASD and Tape capacity along with • A standard set of charts and graphs are prepared to track customer usage • A monthly set of charts are prepared to track customer projections vs. actual usage. • A monthly set of charts (graphic view of Resource Capacity utilization)	2.4 Mainframe Capacity Planning and Management Services ***- Capacity Plan*** ***- Capacity Report***	monthly	1 incl. 22 graphs	Word H/S
Capacity Utilization charts – *"Month/Year"*	A set of charts (graphic view of Resource Capacity utilization) presented by Service Provider to Client forums	2.8 Mainframe Client Technical Support Services	monthly –	20 graphs	Excel S
INFO Reports	A broad range of usage reports, system and client based • primarily text based; some standard graphs	2.9 Mainframe Reporting Support Services	hourly, daily, monthly	Availability: 9 Performance: 17 Client specific: 25 common reports with 21 views Utilization: 14 Graphs: 40 total	TSO/ISPF panels S

Report Name	Description	Link to SOW Section	Frequency	# of Reports (approx.)	Format Hardcopy or Softcopy
				(these graphs can be displayed in z/OS and equivalents of the web site graphs	
Capacity and Performance Graphs	Presents a number of performance and utilization reports, overall and client specific views: URL: https://workplacetechnologyservices.gov.bc.ca/dps/dpsdrpt.html	2.9 Mainframe Reporting Support Services	daily	Dashboard: 4 views Daily: 19 views CICS: 5 views Monthly: 25 views	Web S
Services Volume Utilization Graphs	Used by Province Service Management: - 36 months history - Number of non-scheduled IPLs - A/ D/ I avg. utilization prime shift - A/ D/ I avg. utilization non-prime shift - IMS prod txn volume - IMS2 prod txn volume - IMS Test txn volume - CICS Prod txn volume - CICS Test txn volume - Batch jobs (all classes) txn volume - TSO txn volume - Total no. of TSO sessions - Total no. of tape mounts - Total no. of DB2 threads from IMS - Total no. of DB2 threads from CICS - Total no. of DB2 threads from TSO - Total no. of DB2 threads from Batch - No. of non-silo tape mounts - No. of silo tape mounts	2.9 Mainframe Reporting Support Services	monthly	23 charts	Mainframe H

Report Name	Description	Link to SOW Section	Frequency	# of Reports (approx.)	Format Hardcopy or Softcopy
WWG Mainframe Usage Forecast Worksheet	Excel spreadsheet template – Service Provider maintains the template and supports any required macro changes	2.4 Mainframe Capacity Planning and Management Services	semi-annually	1	Excel S
IFMEARLW/ Monthly Reporting Group MIPS	Resource capacity usage and forecasting – MIPS utilization – data used by Province to populate WWG forecast templates for Clients	2.4 Mainframe Capacity Planning and Management Services	monthly	1	Excel S
IFYACT 18 months – TAPE	Resource capacity usage and forecasting – TAPE utilization – data used by Province to populate WWW forecast templates for Clients	2.4 Mainframe Capacity Planning and Management Services	monthly	1	Excel S
IFYACT 18 months – STC	Resource capacity usage and forecasting – Started tasks – data used by Province to populate WWW forecast templates for Clients	2.4 Mainframe Capacity Planning and Management Services	monthly	1	Excel S
IFYACT 18 months – ACTUALS	Resource capacity usage and forecasting – MIPS, DASD and Tape Mounts – data used by Province to populate forecast templates for Clients	2.4 Mainframe Capacity Planning and Management Services	monthly	1	Excel S
IFYACT 18 months – PRINT	Resource capacity usage and forecasting – PRINT (simplex, duplex, impact counts by Client) – data used by BC Mail Plus	2.10 Mainframe Forms and Print Support Services	monthly	1	Excel S
Accounting Factors: – Impact Analysis	Modeling impact of accounting factor change to assess impact on utilization allocation	2.9 Mainframe Reporting Support Services	3 times prior to Feb	3	Word/Excel S

Report Name	Description	Link to SOW Section	Frequency	# of Reports (approx.)	Format Hardcopy or Softcopy
Accounting Factors: – Supplemental report	Pro forma impact of accounting factor change – for WWG	2.9 Mainframe Reporting Support Services	once per year prior to July forecast update	1	Word/Excel S
HSM Performance Charts	Tape Queue/Recall Performance Measurement	2.9 Mainframe Reporting Support Services	monthly	1	Excel S
DDFIFYACT.XLS	Resource capacity usage and forecasting – spreadsheet of MIPS summary by customer for assessment of new DB2 workload	2.9 Mainframe Reporting Support Services	monthly	1	Excel S
DDFMIPSHISTORY.XLS	Resource capacity usage and forecasting – monthly MIPS history for assessment of new DB2 workload	2.9 Mainframe Reporting Support Services	monthly	1	Excel S
DDFSLASUMMARY.XLS	Resource capacity usage and forecasting – summary by JOB for assessment of new DB2 workload	2.9 Mainframe Reporting Support Services	monthly	1	Excel S
DDFMIPSUSAGE.XLS	Resource capacity usage and forecasting – usage by USERID for assessment of new DB2 workload	2.9 Mainframe Reporting Support Services	monthly	1	Excel S
Mainframe System Software Plan	System Software maintenance and upgrade plan – 18 month view forward – category, description, rationale, benefits, planned implementation date, status, TIB reference, requirement for Client testing	2.2.1 Mainframe System Software Environment Services 2.2.2 Mainframe System Software Preventative Maintenance Services 2.2.3 Software Refresh Services - ***Mainframe System Software Plan***	monthly	1	Excel S

Report Name	Description	Link to SOW Section	Frequency	# of Reports (approx.)	Format Hardcopy or Softcopy
Mainframe Hardware Plan	Hardware maintenance and upgrade plan – 18 month view forward – category, description, rationale, benefits, planned implementation date, status, TIB reference, requirement for Client testing	2.1.1 Mainframe System Hardware Environment Services 2.2.2 Mainframe System Hardware Services 2.1.3 Mainframe Hardware Refresh Services ***- Mainframe Hardware Plan***	monthly	1	Excel S
Storage Utilization Report	Provide high level report of major storage categories with metrics related to configuration diagram	2.9 Mainframe Reporting Services	monthly	under development	TBD
Network Utilization Report	Provide high level mainframe network report on usage statistics and patterns (TCPIP, TN3270, FTP, etc)	2.9 Mainframe Reporting Services	monthly	under development	TBD
TAPE Management Report: – Annual Inventory Report	Results of Annual Tape Inventory	2.3.1 Mainframe Storage Services	annually	1	PDF H/S
TAPE Management Report: – Client Removable Media Report	Tapes sent out of Data Centre	2.3.2 Client Removable Media Management Services	quarterly	1	PDF H/S
TAPE Management Report: – Certificate of Destruction/Tape volume listings	Confirmation list of volume serial numbers of Province tape volumes processed for confidential destruction	As defined in the Security SOW	ad hoc	ad hoc	PDF H
Service Measures Report: - Monthly Report Service Measures Report: – 3 month Summary	detailed Service Measures attainment for previous year, includes: • Production LPARS, IMS Class 1 & 3 timeliness; • Production LPARS, DDF availability & timeliness;	2.9 Mainframe Reporting Services	Monthly high level summary of Service		Word S

Report Name	Description	Link to SOW Section	Frequency	# of Reports (approx.)	Format Hardcopy or Softcopy
	• Production LPARS VTAM, TCP/IP, VPS, DRS outages; and • All of the above on the Development LPAR		Measure attainment by month		

APPENDIX C – MAINFRAME HARDWARE LIST

The Managed Mainframe Services will commence in January 2011. As a result, the Parties acknowledge and agree that the Supplier hardware is expected to change over the period from the signing of the Agreement until January 2011. Mainframe Hardware technology refreshes will be carried out in accordance with Section 2.1.3 (*Mainframe Hardware Refresh Services*) of this SOW. The following list of hardware will need to be verified and possibly modified due to technology changes prior to commencement of Managed Mainframe Services.

Location	Hardware Device	Supplier	Owner	Description
STMS Calgary Data Centre	CPU	IBM	Service Provider	z9 technology (Model 2096-s03) • 617 MIPS, • 16 GB Memory, • 32 FICON Channels, • 32 ESCON Channels, • 8 OSA/E ports
STMS Calgary Data Centre	DASD	EMC	Service Provider	3.525TB Usable DMX-4 • 8GB Global Memory, • 4 FICON, • 73GB Drives
STMS Calgary Data Centre	Tape -VSM	SUN	Service Provider	VSM5 • 16TB Disk Memory, • 16 FICON Channels, • 256 virtual drives
STMS Calgary Data Centre	Tape -SL8500	SUN	Service Provider	Tape Library • 2500 Slots, • 8 Handbots
STMS Calgary Data Centre	Tape -Drives	SUN	Service Provider	(8) 9840D Encryption capable drives
STMS Calgary Data Centre	Tape - KMS Server	SUN	Service Provider	Key Management server for Tape Drive Data Encryption
Disaster	CPU	IBM	SunGard	SUNGARD Shared Service CPU

Location	Hardware Device	Supplier	Owner	Description
Recovery Site				• 8 GB Memory, • 32 FICON Channels, • 8 ESCON Channels, • 4 OSA/E
Disaster Recovery Site	DASD		SunGard	SUNGARD Shared Service disk • 3.525TB Usable, • 8GB Global Memory, • 4 FICON
Disaster Recovery Site	Tape -VSM	SUN	Service Provider	VSM5 • 7.5TB Disk Memory, • 16 FICON Channels,256 virtual drives
Disaster Recovery Site	Tape -SL8500	SUN	Service Provider	Tape Library • 1750 Slots, • 8 Handbots
Disaster Recovery Site	Tape -Drives	SUN	Service Provider	(8) 9840D Encryption capable drives
Disaster Recovery Site	Tape - KMS Server	SUN	Service Provider	Key Management server for Tape Drive Data Encryption

APPENDIX D - MAINFRAME SYSTEM SOFTWARE

Appendix D.1 *Standard Software*

Appendix D.1.1 *Service Provider Provided Base Software*

The Service Provider will provide the following Supplier software products as part of the Standard Software base. License and maintenance fees associated with these products are recovered in the monthly MIPS rate.

Supplier	z/OS Product	Purpose / Description
Computer Associates	CA	S. 15
Computer Associates	CA S. 15	
Computer Associates	CA	
Computer Associates	Multi Image Integrity	
Computer Associates	SMR	
IBM	CICS S. 15	
IBM	DB2 S. 15	
IBM	IMS/ESA S. 15 S. 15	
IBM	S. 15	
IBM	Ent COBOL S. 15	
IBM	ICKDSF	
IBM	JAVA S. 15	
IBM	REXX	
IBM	SD/2 S. 15	
IBM	SMP/E	
IBM	System Automation	
IBM	WebSphere MQ for S. 15	
IBM	WebSphere MQ for	
IBM	z/OS	
IBM	z/OS S. 15	
IBM	z/OS	
IBM	z/OS	

Supplier	z/OS Product	Purpose / Description
IBM	z/OS	S. 15
IBM	z/OS S. 15	
IBM	z/OS	
Innovation	FATS/FATAR	
STK	ExLM	
STK	HSC STK ATL	
Syncsort Incorporated	Syncsort S. 15	

Appendix D.1.2 Service Provider Developed Software

The Service Provider will provide the following developed software products as part of the Standard Software base. The costs for this Standard Software are recovered in the monthly MIPS rate.

Supplier	z/OS Product	Purpose / Description
Service Provider	ATRM	S. 15
Service Provider	CHARMS	
Service Provider	CICS	
Service Provider	CICS S. 15	
Service Provider	CICS	
Service Provider	CICS	
Service Provider	Crystal	
Service Provider	Data Set Update and Display	
Service Provider	Date Manipulation	
Service Provider	DB2	
Service Provider	DB2 S. 15	
Service Provider	S. 15	
Service Provider	Document Facility EDF	
Service Provider	eSMS	
Service Provider	FZAP S. 15	
Service Provider	GRS S. 15	
Service Provider	Hold Job S. 15	
Service Provider	IMS S. 15	

Supplier	z/OS Product	Purpose / Description
Service Provider	IMS Utilities	S. 15
Service Provider	IPCS	
Service Provider	JCS2 S. 15	
Service Provider	JES2	
Service Provider	MOM	
Service Provider	MPF Exits S. 15	
Service Provider	Multi DB2	
Service Provider	MVS	
Service Provider	MVS S. 15	
Service Provider	MXI	
Service Provider	NPL S. 15	
Service Provider	Online Notification S. 15	
Service Provider	PAM	
Service Provider	PDS S. 15	
Service Provider	Problem Change Collection Tool S. 15	
Service Provider	PRO-J	
Service Provider	S. 15 DB2	
Service Provider	Reusable Programs	
Service Provider	Reusable Subs & Macros	
Service Provider	SAM S. 15	
Service Provider	SCM & Re-Engineering Support	
Service Provider	Service Excellence Dashboard	
Service Provider	S. 15 MVS	
Service Provider	SME	
Service Provider	SOS	
Service Provider	SP Tools S. 15	
Service Provider	Standard S. 15	
Service Provider	Transparent Loaders	
Service Provider	Unicenter CA S. 15	
Service Provider	S. 15	

Appendix D.2 *Non-Standard Software*

Appendix D.2.1 *Service Provider Provided, Province Paid Software*

The Service Provider will provide the following Supplier software products as part of the Non-Standard Software. The costs for the Non-Standard Software are recovered in the monthly Non-Standard software charge. The Parties acknowledge that the fees associated with the Non-Standard Software products provided by the Service Provider may be amended to reflect a change in hardware technology if there is a requirement to move from z9 to z10 as reflected in Appendix C – Hardware List.

Note: The Non-Standard software monthly fee is adjusted annually by the Service Provider. The fee will increase or decrease to reflect changes in supplier maintenance fees and changes in CPU capacity and / or software mix.

Supplier	z/OS Product	Purpose / Description
BMC Software	CMF	
BMC Software	Delta S. 15	
BMC Software	ETA	
BMC Software	S. 15 IMS	
BMC Software	MAINVIEW	
BMC Software	MAINVIEW	
BMC Software	MAINVIEW S. 15	
BMC Software	MAINVIEW	
BMC Software	MAINVIEW	
BMC Software	MAINVIEW	S. 15
BMC Software	MAINVIEW S. 15	
BMC Software	MAINVIEW	
BMC Software	MAINVIEW	
BMC Software	MAINVIEW	
BMC Software	S. 15 IMS	
Chicago Soft Inc	MVS S. 15	
Computer Associates	S. 15	
Computer Associates	CA S. 15	
Computer Associates	BATCH PROCESSOR	
Computer Associates	S. 15	

Supplier	z/OS Product	Purpose / Description
Computer Associates	ESP	S. 15
Computer Associates	ESP	
Computer Associates	PDSMAN	
Computer Associates	TSO	
Computer Associates	XCOM	
Computer Associates	XMANAGER	
S. 15	S. 15	
SAS Institute (Canada) Inc.	SAS	
SAS Institute (Canada) Inc.	SAS	
SAS Institute (Canada) Inc.	SAS	
SAS Institute (Canada) Inc.	SAS	
SAS Institute (Canada) Inc.	SAS	
SAS Institute (Canada) Inc.	SAS	
Syncsort Incorporated	MVS	

Appendix D.2.2 Province Provided Software

The Province will provide the Service Provider with use and access rights to the following Supplier software products and they are categorized as Non-Standard Software.

Vendor	z/OS Product	Purpose / Description
Allen Systems Group	Docutext	S. 15
Allen Systems Group	Pro/JCL	
Allen Systems Group	ViewDirect for MVS	
Canada Post/CPC Data Licensing	Directories of Postal Codes	
Compuware Corporation	Abend	
Compuware Corporation	Abend	
Compuware Corporation	ECC -	
Compuware Corporation	ECC -	
Compuware Corporation	ECC -	
Compuware Corporation	ECC -	
Compuware Corporation	Fileaid	
Compuware Corporation	Fileaid	

Vendor	z/OS Product	Purpose / Description
Compuware Corporation	FileAid	S. 15
Compuware Corporation	Fileaid/	
Compuware Corporation	Fileaid/	
Compuware Corporation	Fileaid/	
Compuware Corporation	Fileaid/	
Compuware Corporation	Fileaid/	
Fischer International Systems	IOF	
IBM	AFP Font Collection	
IBM	ASF - Doc Composition Feature	
IBM	BARCODE	
IBM	Batchpipes	
IBM	CCCA S. 15	
IBM	DCF	
IBM	DCF DLF	
IBM	Debug Tool S. 15	
IBM	Enterprise S. 15	
IBM	Fonts	
IBM	Fonts	
IBM	Fonts - Son Sans 3820	
IBM	Fonts - Son Serif 3820	
IBM	Fonts - Son S Ser HD3820	
IBM	Fonts - Son Serif HD3820	
IBM	Host Command Facility	
IBM	IMS S. 15 S. 15	
IBM	S. 15	
IBM	IMS S. 15 S. 15	
IBM	IMS S. 15	
IBM	InfoPrint Transforms	
IBM	ImagePlus Object Distribution Manager (IODM)	

Vendor	z/OS Product	Purpose / Description
IBM	ImagePlus S. 15 S. 15	
IBM	NCP	
IBM	NCP	
IBM	NCP S. 15	
IBM	NCP	
IBM	NCP	
IBM	Netview S. 15	
IBM	OGL S. 15	
IBM	PL/I S. 15	
IBM	PPFA S. 15	
IBM	S. 15	
IBM	PSF	
IBM	PSF S. 15	
IBM	PSF	
IBM	PSF	
IBM	QMF	S. 15
IBM	SDF S. 15	
IBM	SDF	
IBM	VisualAge S. 15	
IBM	XML	
IBM	z/OS	
IBM	z/OS S. 15	
IBM	z/OS	
IBM	z/OS	
IBM	z/OS	
IBM	z/OS	
IBM	z/OS S. 15	
IBM	z/OS	
IBM	z/OS	
IBM	z/OS	
Innovation	FDR	

Vendor	z/OS Product	Purpose / Description
Levi, Ray & Shoup, Inc.	DRS	
Levi, Ray & Shoup, Inc.	VPS	
Levi, Ray & Shoup, Inc.	VPS S. 15	
Merrill Consultants	MXG	
MVS Solutions Inc.	Thruput Manager	
MVS Solutions Inc.	Thruput Manager S. 15	
MVS Solutions Inc.	Thruput Manager	S. 15
Open Software Technologies Inc.	Rexx Tools	
Open Software Technologies Inc.	Rexx Tools S. 15	
Open Software Technologies Inc.	REXXtools	
SumTotal	Preference Library & Preference S. 15	
Prism Data Services	Dr. Q	
Software Engineering of America	PDSFAST	
SPSS Inc.	SPSS STAT	

Appendix D.2.3 Province Developed Software

The Province will provide the following Province Developed Software as part of the Standard Software base. The Service Provider may use the Province Developed Software. The maintenance and support for this Province Developed Software is recovered in the monthly MIPS rate.

Supplier	z/OS Product	Purpose / Description
Province	S. 15	S. 15
Province	Service Request System	
Province	Custom code – print services and support	
Province	Custom code – operating system software	

APPENDIX E – AUTHORIZATIONS

Section	Authorization Description	Authorized personnel
1.15	Batch Schedule Approval	Managed Mainframe Services related Authorization lists will be provided as part Mainframe Transformation as documented in the Transformation SOW
2.3.2	Client Removable Media Support Services	Managed Mainframe Services related Authorization lists will be provided as part Mainframe Transformation as documented in the Transformation SOW

STMS Hosting Services

SOW 5A

Server Management Services

TABLE OF CONTENTS

S. 15

1. SOW 5A, Scope and Summary

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in Appendix A of this SOW, the Agreement and the Master Transfer Agreement, as applicable.

1.2 Purpose of this Document

1.2.1 General

The purpose of this SOW is to describe the scope and functions of the Server Management Services to be performed by Service Provider for the Province under the terms of the Agreement, and the general provisions that will apply to this SOW and the Supporting SOWs. This SOW sets forth the background and a general overview of the Server Management Services in Section 1.3 (*Server Management Services Overview*) below, and describes the Server Management Services in more detail in Section 1.4 (*Server Management Services Description*) below.

1.2.2 Outcomes Based Approach

The services described in this SOW and in the Supporting SOWs use an outcomes-based approach. The outcomes-based approach used to describe the services in this SOW and the Supporting SOWs is intended to allow Service Provider the ability to determine the most efficient manner of providing the services so described while achieving all applicable Service Levels; provided that in providing the Services under this SOW and the Supporting SOWs the Service Provider complies, at all times, with the Privacy Obligations, the requirements of the Security SOW and the Province Security Policies & Standards (as defined in the Security SOW).

Accordingly, the specific procedures, processes and associated tasks required to be undertaken by Service Provider to perform the Services under this SOW and the Supporting SOWs are not described in this SOW and in the Supporting SOWs, but will be described more fully in the Midrange Operating Manual (defined below). As a result, it is the intention of the Parties that Service Provider will do what is required to deliver the Services under this SOW and the Supporting SOWs in compliance with the requirements of this SOW and the Supporting SOWs, even though the specific procedures, processes and tasks to do so are not specifically identified or otherwise articulated; provided that in doing so the Service Provider shall not be responsible for (or otherwise be required to undertake) those matters that are specified in this SOW, the Supporting SOWs or elsewhere in the Transaction Documents as being the responsibility of the Province, a Client or a third party (where the third party is not a Subcontractor of Service Provider for purposes of providing Services under the Agreement).

1.2.3 Responsibility Charts

Section 1.4 (*Server Management Services Description*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the

Server Management Services, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.2.4 Midrange Operating Manual

For greater clarification, it is the intention of the Parties that the specific procedures, processes, tasks and functions not described in this SOW or in the Supporting SOWs that are required to be performed by Service Provider in order to deliver the Services under this SOW and the Supporting SOWs shall be described in detail in an operating manual (the "**Midrange Operating Manual**"), to be prepared by Service Provider as part of the transformation activities under the Transformation SOW. The Midrange Operating Manual shall form part of the Manual described in Sections 4.8 (*Documentation*) and 4.9 (*Manual Requirements*) of the Agreement. Service Provider will provide the Province with a copy of the Midrange Operating Manual upon request from time to time.

The Parties acknowledge that on the Hand-Over Date, the Midrange Operating Manual shall consist of the processes, procedures (and associated tasks and functions) that are in use by the Province immediately prior to the Hand-Over Date (the "**Province Procedures**") until the Province Procedures have been revised by Service Provider as contemplated in the Transformation SOW. The Parties acknowledge that the Province Procedures are in various states of completion and drafting, and will not necessarily articulate all processes, procedures, tasks and functions that will be required for Service Provider to provide the Services under this SOW and the Supporting SOWs immediately following the Hand-Over Date.

1.2.5 Server Locations, Transformation and Ownership

Transformation

As of the Hand-Over Date, the Servers that are the subject of the Services under this SOW and the Supporting SOWs are located at Remote Sites, Province Data Centres and Regional Network Centres. As part of the Transformation SOW and the Annual Operating Plan, the Province Data Centres will be (and some Remote Sites and Regional Network Centres may be) decommissioned in whole or in part and replaced by the STMS Data Centre. The Services under this SOW and the Supporting SOWs in respect of the Servers located at the Province Data Centres (and such Regional Network Centres and Remote Sites) may change as a result of the decommissioning of Province Midrange Facilities, and any such changes shall be documented as part of the transformation activities described in the Transformation SOW or the planning activities of the Annual Operating Plan.

Ownership

Regardless of the location of any Servers that are the subject of the Services under this SOW or the Supporting SOWs, the Province Owned Equipment and all additions and upgrades to the Province Owned Equipment shall at all times be and continued to be owned by the Province, and

the Service Provider Owned Equipment and all additions and upgrades to the Service Provider Owned Equipment shall be and continue to be owned by Service Provider, unless and until such Service Provider Owned Equipment is purchased by the Province in accordance with Section 29.6 (*Transfer of Assets, Contracts and Software*) of the Agreement.

1.2.6 Storage and Cabling

Service Provider will be responsible for network and storage cabling from the Province network switch in the Remotes Sites and Regional Network Centres. Cabling provided in the STMS Data Centre and in the Province Data Centre is described in Data Centre SOW.

1.2.7 Use Rights & Support Agreements

Use Rights

The parties acknowledge that there are certain software licenses and software and hardware maintenance agreements as listed in a Schedule to the Master Transfer Agreement (referred to in this SOW and in the Master Transfer Agreement as the "**Access Rights Contracts**"), that will be maintained by the Province and used by the Service Provider in performing the services under this SOW and the Supporting SOWs in respect of the Province Owned Equipment and the Province Licenses. Unless otherwise determined under the Change Order Process or the Change Management Process, as applicable, the Province will grant the Service Provider access and use rights to the Access Rights Contracts as set forth in the Master Transfer Agreement (the "**Use Rights**"), and will maintain the Access Rights Contracts in good standing for that purpose. The provisions of the Master Transfer Agreement will apply in respect of the Access Rights Contracts and the Use Rights. Service Provider and Province will exchange and provide information to each other as may be necessary to facilitate the Use Rights and to maintain the Access Rights Contracts in good standing.

Microsoft Licenses

Notwithstanding the above, the Service Provider will obtain its own Microsoft "premier support maintenance agreements" for the Microsoft licences provided by the Province, and accordingly, the Use Rights will not apply to support agreements for Microsoft Software included in the Province Licenses (the "**Microsoft Licenses**"). For greater clarification the Province will provide use rights to the Service Provider for the use and maintenance of the Microsoft Licenses.

Non-Maintenance Equipment/Software

Except as set forth above regarding the Microsoft Licenses, if any Province Owned Equipment or Province Licenses are not subject to any Access Rights Contracts (the "**Non-Maintenance Equipment and Software**"), then: (1) the Service Provider will use reasonable commercial efforts to resolve Problems and Incidents relating to the Non-Maintenance Equipment and Software; (2) as long as the Service Provider uses such reasonable commercial efforts, it will be relieved from applicable Service Levels in respect of the Non-Maintenance Equipment and Software if it is unable to resolve the Problems and Incidents; and (3) the Service Provider will

work cooperatively with the Province to determine how to resolve such Problems and Incidents, and if necessary, the matter will be resolved through the Governance Process.

To the extent that a software licence, or a software or hardware maintenance agreement in addition to the Access Rights Contracts is required by the Service Provider to perform the services under this SOW or the Supporting SOWs, then unless otherwise determined under the Change Order Process or the Change Management Process, as applicable, the Service Provider will obtain and maintain such licences and maintenance agreements as required to perform the applicable services. These will include, without limitation, the Operating Systems supplied with the Service Provider Owned Equipment, the Service Provider Tools, and software required for the Virtual Servers (as described in the Virtual Server SOW).

1.2.8 Use of Province Ordering System, ITIMS and Request Management

The use of ITIMS and Request Management in this SOW refer to the processes more fully described in the Services Management SOW. The use of Province Ordering System in this SOW is described at a high level and is more fully described in the Services Management SOW and the Manual (as defined in the Agreement).

1.2.9 Appendices

The following Appendices are attached to and form part of this SOW, whether or not they are specifically referred to in this SOW:

- Appendix A – Defined terms/Definitions
- Appendix B – Midrange Reports
- Appendix F – Supported Operating Systems
- Appendix G – Managed Services – Storage of Surplus Hardware
- Appendix H – Province Ordering System Process Flow
- Appendix I – Major Midrange Software Release Upgrades
- Appendix J – Server Technology Evolution

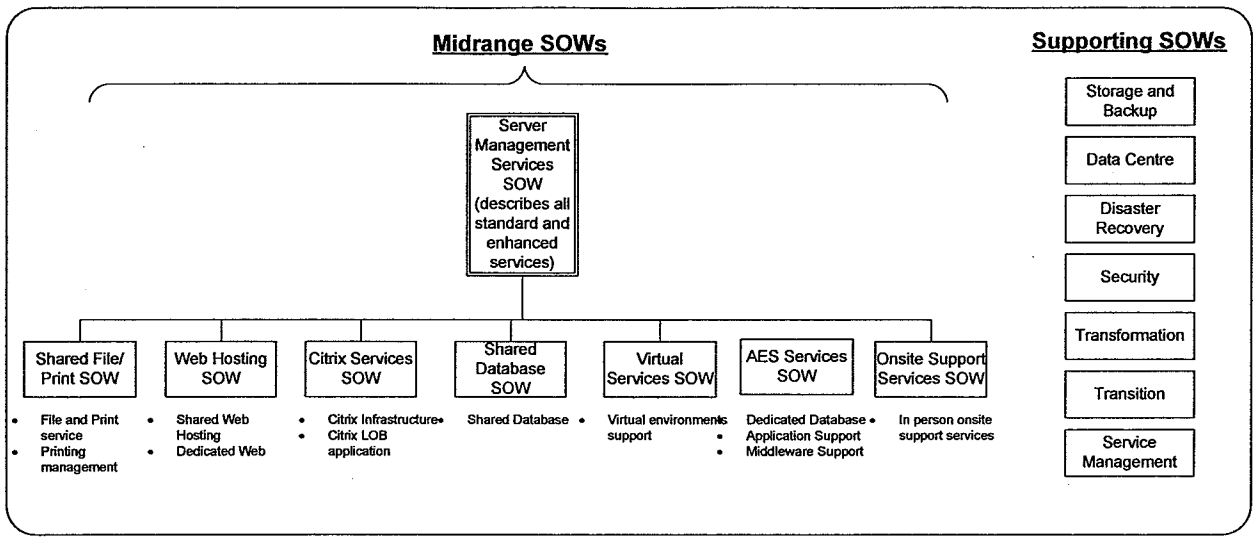
1.3 Server Management Services Overview

1.3.1 Background

The Server Management Services provides for the deployment and daily delivery of Server hosting and management services to the Province (and Clients) consisting of procuring, installing, configuring, maintaining, upgrading, decommissioning and disposing of Servers and Server-related hardware, firmware, Operating Systems, backup and restore software, security software and monitoring software (such as anti-virus software, Server availability monitoring, Server performance monitoring), all as more particularly described in this SOW and in the documents referred to in this SOW.

The components of the Server Management Services described in this SOW apply to all Servers referred to in the other "Midrange SOWs", as illustrated in the diagram below. The Services described in other "Midrange SOWs" (which are referred to in the diagram below as

"**Supporting SOWs**") are dependent upon the services described in this SOW. The Supporting SOWs are cross -referenced in this SOW.



1.3.2 Server Management Services Components - General Overview

The Server Management Services are broken down into the components listed below (each of which are described more fully in Section 1.4 (*Server Management Services Description*)), and generally follow the lifecycle of a Server. The Parties acknowledge that the Server Management Services provided by Service Provider on the Province Owned Equipment will apply, as required, given the stage that each Province Owned Server is at in its lifecycle (for example, if a Province Owned Server has been procured but not installed on the Hand-Over Date, then it will be the subject of the "Hardware Installation Services", but not necessarily the "Server Procurement Services" described in this SOW).

The components of the Server Management Services listed below as "Standard" (and further described in this SOW) apply to all of the Province Owned Equipment and all Service Provider Owned Equipment, whether located at the Province Data Centres, the Remote Sites, the Regional Network Centres or the STMS Data Centre.

The Server Management Services listed below and described in this SOW as "Optional" are optional services that can be provided by Service Provider to the Province and Clients upon request through Province Ordering System at the discretion of the Province and Clients (and will be offered through Province Ordering System at such times as may be determined by the Province). For greater clarification, the "Optional" Server Management Services may also be purchased by the Clients from a different vendor, and need not be purchased from the Service Provider.

Standard Server Management Services Components

- Province Ordering System Process
- Midrange General Responsibilities

- Reporting
- Privileged Account Management
- Server Procurement
- Server Hardware Installation
- Server Operating System Installation and Configuration
- Server Hardware Fault Management
- Operating System Support and Fault Management
- Patch Management
- Server Hardware Upgrading and Replacement
- Server Operating System Upgrading
- Regular and Ongoing Client Interaction
- Remote Server Support
- Image Performance Management Services
- Server and Equipment Decommission
- EnCase

Optional Server Management Services

- Image Performance Management – Optional Services
- Server Capacity – Optional
  - A per Server charge for adding Server Capacity – Optional to a Server.

- Cluster Management – Optional
  - A per Server charge for adding Cluster Management – Optional to a Server.

- Application Monitoring Services – Optional
  - A per Server charge for adding Application Monitoring Services – Optional to a Server. Monitored against Client specified measures and thresholds for the purpose of Application event notifications and escalations.

- Batch Management Services – Optional
  - A per Server charge for adding Batch Management Services – Optional to a Server or Servers.

- Extended Support Hour Uplift - 5 x 12
  - A per server charge for increasing server management hours from 5 x 9 to 5 x 12.

- Extended Support Hour Uplift - 7 x 24
  - A per server charge for increasing server management hours from 5 x 9 to 7 x 24.

- Extended Support Hour Uplift - Remote - 7 x24
  - A per server charge for increasing remote (i.e. Non-data centre locations) server management hours from 5 x 9 to 7 x 24.

1.4 Server Management Services Description

The parties intend that as the Province Owned Equipment is retired and decommissioned in the ordinary course and as a result of the Transformation of the Services, it will be replaced with Service Provider Owned Equipment.

The Server Management Services under this SOW may be purchased by the Province and by Clients in different Tiers, as described below, where each Tier provides a different level of service package. For greater clarification, the Tiers described below do not apply to the services provided under the Supporting SOWs unless expressly provided otherwise in the Supporting SOWs.

- Tier 1 - Business Priority - geographically distributed Server cluster with synchronous data replication:
  - Available as a geographically dispersed cluster with synchronous data replication
  - Available as a cluster across two separate data Centres
  - 7 x 24 support
  - Cluster Management - Requires at least two Servers

- Tier 1 - Business Priority - geographically distributed Server cluster with asynchronous data replication
  - Available as a geographically distributed Server cluster with asynchronous data replication
  - Available as a cluster across two separate data Centres
  - 7 x 24 support
  - Cluster Management - Requires at least two Servers

- Tier 1 - Business Priority - Clustered in a single data Centre location
  - Available as a cluster within a single Province Data Centre or STMS Data Centre
  - 7 x 24 support
  - Cluster Management - Requires at least two Servers

- Tier 2 - General Business Base – Data Centre
  - Single hosted Server
  - Province Data Centre or STMS Data Centre locations only
  - 3 month commitment on Virtual Servers
    - Virtual Servers automatically recover upon host or Image failure
  - There are different support hours options available for Tier 2: 5x9, 5x12, 7x24

- Tier 3 - Remote Individual Server
  - Single hosted Server
  - Remote locations and Regional Network Centre (non-Data Centre locations)
  - 3 month commitment on Virtual Servers
    - Virtual Servers automatically recover upon host or Image failure
  - There are different support hours options available for Tier 2: 5x9, 7x24

- Development / Test Servers
  - Single hosted Server for the delivery of testing or development of Client Applications
  - 3 month commitment on Virtual Servers
  - Virtual Servers automatically recover upon host or Image failure
  - There are different support hours options available for Development / Test Servers: 5x9, 7x24

1.4.1 Province Ordering System Process

The Province Ordering System process that will be followed by the Parties under this SOW and the Supporting SOWs (the "**Province Ordering System Process**") is described more fully in the Responsibility chart below, and is further illustrated in the diagram attached as Appendix H

Province Ordering System Process	Province	Service Provider
The Province or Client, as applicable, will initiate a service request that may become a Province Ordering System order.	R	
The Client will submit the service request into Province Ordering System where the Client has sufficient knowledge to do so without further consultation.	R	
Where the Client does not have sufficient knowledge to submit a service request into Province Ordering System without further consultation, the Province's "Integrated Service Solutions Branch" (**ISS**) will facilitate consultations among the Client, the Province, the Province (EHS), the Service Provider and such other parties that may be determined by the Province, to clarify the Client's business requirements and the particulars of the Client's service request that may become a Province Ordering System order (the "**Consultations**").	R	
Service Provider will work with the Province to provide feedback and clarification as part of the Consultations by providing the following: • a knowledgeable subject matter expert with appropriate expertise to advise the Client and the Province in respect of the Client's business requirements and the appropriate technical solution for dealing with those business requirements; • recommendations for an appropriate technical solution for dealing with the Client's business requirements and based		R

upon the Manage Service Catalogue, and where recommendations cannot be made based upon the Manage Service Catalogue then the recommendations will be based upon a special or customized order; • a quote of the cost of the recommendations made by the Service Provider (which quote will only be provided to the Province (EHS), and not to the Client directly), if requested by the Client or by the Province; and • instructions to the Client regarding how to submit the service request into Province Ordering System.		
At the Client's discretion, the Client will submit the service request into Province Ordering System based upon the Consultations and upon the instructions received from the Service Provider.	R	
The Province (EHS) will validate all Province Ordering System orders before they receive financial approval from the Client (the "**EHS Validation**"), and for those orders that were quoted by the Service Provider, the Province (EHS) will enter a price into Province Ordering System based upon (but not less than) the quote from the Service Provider (and for greater clarification, the price so entered into Province Ordering System may include a margin determined by the Province to be paid by the Client to EHS).	R	
The Client will provide financial approval for all Province Ordering System orders entered into Province Ordering System before they are processed by the Service Provider.	R	
Service Provider to fulfill the service requested through the final and financially approved Province Ordering System order.		R

1.4.2 Midrange General Responsibilities

The Midrange General Responsibilities component of the Server Management Services describe general responsibilities of the Service Provider and Province relating to the Server Management Services, and is described more fully in the Responsibility chart below, and include the following:

- Architecture and design of the Server hardware and the Server Management Services.
- Management of maintenance contracts and third party vendor relationships.
- Creation and maintenance of Midrange Operating Manual.
- Privileged access for creation and maintenance of Server accounts, as required for Service Provider to perform the Services.

- Standard maintenance windows.
- Server certification criteria.
- Compliance with location based guidelines for Province Midrange Facilities.

Midrange General Responsibilities	Province	Service Provider
The Service Provider and the Province will, through the Joint Technical Architecture Governance Committee, and subject to the Privacy Obligations, the Security SOW, the Province Security Policies & Standards and any Province CIO direction or guidelines, jointly determine the architecture and design for the following midrange services (the "**Midrange Architecture**"), and where the Joint Technical Architecture Governance Committee is unable to reach agreement on any matter it will be referred to the Joint Operating Committee:		
• Servers		
• Operating system		
• Related monitoring systems		
• Shared File Services		
• Shared Print Services		
• Shared Database Services		
• Shared Web Services		
• Citrix Application Hosting Services		
• Virtual Server Hosting Services	R	R
The Province will approve the Midrange Architecture where it could have an effect or other impact on the Province and will notify the Service Provider through the Joint Technical Architecture Governance Committee where such approval is not required.	R	
Service Provider will create, update and maintain documentation (to the standard required under the Agreement) that describes the agreed Midrange Architecture.		R

Midrange General Responsibilities	Province	Service Provider
Service Provider will establish standard Server maintenance windows for the purpose of system maintenance activities as per Appendix G of the Services Management SOW.		R
Service Provider will approve standard Server maintenance windows.	R	
Service Provider will establish non-standard Server maintenance windows for Clients who are unable to utilize existing standard maintenance windows as a result of business requirements as per Appendix G of the Services Management SOW.		R
The Province will approve non-standard maintenance windows	R	
Service Provider will be responsible for all maintenance required to be performed on Service Provider Owned Equipment and Province Owned Equipment, and all related firmware and Operating Systems		R
The Province will provide the Service Provider with Use Rights under the Province's maintenance contracts for Province Owned Equipment.	R	
Service Provider will enter into and maintain vendor maintenance contracts for Service Provider Owned Equipment.		R
Service Provider will comply with Province guidelines and applicable operational procedures when providing services in Province Midrange Facilities.		R
Province will provide Service Provider with guidelines and applicable operational procedures for Province Midrange Facilities.	R	
Province will provide required training to Service Provider Personnel who will be performing services in a Regional Network Centre	R	
Service Provider will ensure its Personnel who will be performing services in a Regional Network Centre to take the "Regional Network Centre" training.		R
Province will provide required "Regional Network Centre" training to Service Provider Personnel.	R	
Servicer Provider will provide to the Province the Server certification criteria to be used by the Service Provider and all amendments and updates to the Server certification criteria prior to their use.		R

Midrange General Responsibilities	Province	Service Provider
Provide space at S. 15 as described in the License Agreement.	R	
Service Provider will provide the cables (such as Network, storage, power and Keyboard Video Mouse (KVM)) required for Service Provider Owned Equipment and Province Owned Equipment.		R
Service Provider will create, manage and remove OpenVMS batch queues as required for Clients.		R
Clients manage and monitor their own batch jobs in the Service Provider OpenVMS batch queues.	R	
Client will, at their discretion, S. 15 to manage OpenVMS batch jobs.	R	
Service Provider will provide 2nd level support as required by the Clients S. 15 to manage OpenVMS batch jobs.		R

1.4.3 Reporting

The Reporting component of the Server Management Services describes general responsibilities of the Service Provider to provide reports to the Province in respect of the Services performed under this SOW.

Reporting	Province	Service Provider
Service Provider will provide the Province with web based access to the performance and availability reports described in Appendix B ("**Reports**"), at the times and frequency set forth in Appendix B, for sharing with Clients as the Province determines.		R
The Service Provider will maintain a twelve month history of the Reports on its web based reporting system.		R
Web based reporting system is operated to meet a "7x24" schedule that allows for reasonable downtime for the Service Provider to perform maintenance as the Service Provider deems reasonably necessary.		R

1.4.4 Privileged Account Management

The Privileged Account Management component of the Server Management Services describes general responsibilities of the Service Provider and Province relating to the granting of Privileged Accounts and the policies related to Privileged Accounts as part of the Server Management Services.

The objective of the Parties is to reduce the level of privilege in the Client Privileged Accounts to a level of Least Privileged Access. The Parties will review the progress of moving towards the Least Privileged Access, and the reduction in the number of Client Privileged Account related Incidents, with the first review being six months after the Hand-Over Date and annually afterwards. The Service Levels will continue to apply in accordance with their terms as the Parties move towards the use of Least Privileged Access.

The Parties will work together to encourage Clients with Client Privileged Accounts to provide the Service Provider with advance notice of significant changes made with their Privileged Accounts (such as Server outages).

Privileged Account Management is more fully described in the Responsibility chart below.

Privileged Account Management	Province	Service Provider
Service Provider will assume responsibility for the existing Province Servers as configured with the existing Privileged Accounts at Hand-Over Date.		R
Province will annually review the Client Privileged Accounts with the Clients. Province will work with the Clients on an annual basis and at other appropriate opportunities (such as Server refresh, Application upgrade, Server virtualization and so on) with the objective of reducing privileges in the Client Privileged Accounts to a level of Least Privileged Access over time, as determined appropriate by the Province.	R	
Within 18 months after Hand-Over Date, the Service Provider will propose tools for Province approval to enhance the Service Provider's ability to identify the root cause of Incidents resulting from the use of Client Privileged Accounts. Any approved tools will be implemented through the Change Management Process.		R
Service Provider will perform root cause analysis to determine if Incidents are a result of the use of Client Privileged Accounts.		R

Privileged Account Management	Province	Service Provider
Service Provider will provision Unix, Linux and OpenVMS privileged accounts in accordance with the Midrange Operating Manual.		R
Province will provision Windows Domain Level Privileged Accounts to Service Provider and others as required.	R	
Province will give sufficient privileged access to the Service Provider to manage Province Privileged Accounts that are local to Servers or that reside in the Province's Windows Domain.	R	
Province (EHS) will put in requests for Privileged Accounts through Request Management Process as described in the Services Management SOW.	R	
Service Provider will create, manage (such as reset passwords, change group membership and so on), and delete accounts with privileged access to Servers (including Client Privileged Accounts and accounts Least Privileged access) through Request Management Process as described in the Services Management SOW.		R

1.4.5 Server Procurement

The Server Procurement component of the Server Management Services describes the procurement of Server hardware and software by Service Provider under this SOW. The Server Procurement component of the Server Management Services is described more fully in the Responsibility chart below.

Server Procurement	Province	Service Provider
Province or Client, as applicable, initiates a service request for Server hardware and software available under the services pursuant to the Province Ordering System Process.	R	
As part of the EHS Validation, the Province (EHS) will: • Verify Server hardware and operating system required and Server configuration and finalize requirements for the Server(s) with the Province.	R	

Server Procurement	Province	Service Provider
• Provide recommendations based on the Manage Service Catalogue or pursuant to a special order. • Provide system specifications of the requested Server for verification against the Province's application requirements.		
Service Provider will receive hardware and software ordered through Province Ordering System and procured by Service Provider (and hardware and software procured by Province prior to the Hand-Over Date that is not delivered to Province before the Hand-Over Date).		R
Service Provider will arrange to receive and store equipment in a secure location for installation at Remote Sites and Regional Network Centres.		R
Service Provider will update the Service Provider Asset Management system as determined by the Services Management SOW.		R
Service Provider to verify completeness of hardware and software received, and provide Province all packing slips for, Province Owned Equipment.		R

1.4.6 Server Hardware Installation

The Server Hardware Installation component of the Server Management Services describes the installation of Server hardware by Service Provider under this SOW. Service Provider will be responsible for the installation of Province Owned Equipment and for the installation of Service Provider Owned Equipment. The Server Hardware Installation component of the Server Management Services is described more fully in the Responsibility chart below and includes the following:

- receipt and storage of hardware by Service Provider;
- Province procedures for hardware installation in Province Midrange Facilities;
- updating of Service Provider asset management systems; and
- notification to Province that hardware installation is complete.

Server Hardware Installation	Province	Service Provider
For hardware installation in Province Midrange Facilities, Province will supply all prerequisite Server environmental services such as power, networking, server rack and, where applicable in the Province Midrange Facilities, cooling and provide all Province Midrange Facility procedures relating to the installation of Servers.	R	
For each Province Midrange Facility, Province will supply access to such Province Midrange Facility as requested by Service Provider to provide services. Province will provide an escort where required for access.	R	
Province will provide training to Service Provider on how to access the Province's Regional Network Centre.	R	
Service Provider will inform the Province of the Service Provider personnel to attend the Province's Regional Network Centre training.		R
Service Provider will attend the Province supplied training on how to access the Province's Regional Network Centre.		R
Service Provider to inform the Province of Service Provider personnel who will attend Province Midrange Facilities for Province approval.		R
Service Provider will install Servers, including: • assemble Server and install into Server rack; • install cables for power, network and storage; and • perform diagnostic tests of Server hardware and peripherals to determine functionality.		R
Service Provider will remove all packing material and any other related material from the Province Midrange Facilities.		R
Service Provider will submit ITIMs Network switch port Request for all Servers within Province Midrange Facilities.		R

Server Hardware Installation	Province	Service Provider
Province will supply network switch information for which port the Service Provider will attach the Server to the Province network (SPAN/BC).	R	
Service Provider will update Service Provider Asset Management system with location information.		R
Service Provider to notify Client that Server hardware installation is complete for Client ordered hardware upgrade.		R

1.4.7 Server Operating System Installation and Configuration

The Server Operating System Installation and Configuration component of the Server Management Services describes the installation of the Operating System on Province Owned Equipment (whether procured by the Province prior to the Hand-Over Date or by Service Provider after the Hand-Over Date) and on Service Provider Owned Equipment. Should the Service Provider software tools interfere with the Client Applications or the operation of the Servers, then the Province and Service Provider will work cooperatively to resolve through Problem Management Process as described in the Services Management SOW. The Server Operating System Installation and Configuration component of the Server Management Services is described more fully in the Responsibility chart below and includes the following:

- supply of configuration elements required by Service Provider to complete the Operating System installation;
- Operating System configuration;
- installation of Operating System as per the Midrange Operating Manual;
- installation and registration of Service Provider Tools on all Province Owned Equipment and all Service Provider Owned Equipment;
- Service Provider certification of Operating System; and
- Service Provider to update Province Ordering System following completion of installation service.

Server Operating System Installation and Configuration	Province	Service Provider
Province will supply configuration elements to Service Provider as required for Service Provider to complete installations such as: • Server name • Associated Province directory services systems • User IDs • User Security Access • Storage partition information • Internet Protocol address information • Required information to align with Security SOW • File system security settings • Initial application administration ID Requirements (such as who the lead administrator is, their network ID and required Server access level)	R	
Province will supply Service Provider with Internet Protocol (IP) address pool range to address Servers which may be given as blocks of Internet Protocol addresses, or IP single addresses as determined by Province.	R	
Service Provider will install Operating System and configure Server based on configuration elements received from the Province.		R
Service Provider will install, configure, test and register Service Provider software tools on Service Provider Owned Equipment and Province Owned Equipment as determined by Service Provider to meet Service Levels and service obligations. Software tools will include: • monitoring agents • automation agents		R

Server Operating System Installation and Configuration	Province	Service Provider
• backup agents • scheduling agents • Anti-malware software		
Service Provider will use existing Province software tools on Province Owned Equipment following the Hand-Over Date until Service Provider software tools are installed in accordance with the Transformation SOW.		R
Province will supply Service Provider with access and training to the Province owned server registration tool (for example the Network Node Registry) as required.	R	
Register Server in Province's server registration system (DNS) following Province procedures and using Province owned tools. (On Hand-Over Date, Service Provider will use the Province's Network Node Registry/Server name Registry tool.)		R
Province will provide Service Provider with either access to Province directory systems for Server registration, or a Province process to be followed to enable the Province to register the Server in the Province directory systems.	R	
Service Provider will register Server into Province directory systems, or follow the Province process to be followed to enable the Province to register the Server in the Province directory systems, as applicable.		R
Service Provider will schedule and configure backups in accordance with Managed Storage and Backup Services SOW.		R
Service Provider will perform Server certification validation and provide a copy to the Province (EHS) upon completion.		R
Service Provider will update Service Provider's Asset Management system.		R
Service Provider will notify the Province (EHS) and the Client that the Server is available for Application installation and configuration by the Province or Client.		R

Server Operating System Installation and Configuration	Province	Service Provider
Service Provider will update Province Ordering System as per the Services Management SOW.		R

1.4.8 Server Hardware Fault Management

The Server Hardware Fault Management component of the Server Management Services describes Service Provider's responsibility to detect, escalate, resolve and perform root cause analysis (as described in the Services Management SOW) in respect of Server hardware (including firmware) faults, and to perform preventive maintenance on the Server hardware as may be necessary for Service Provider to achieve all applicable Service Levels. The Server Hardware and Image Fault management component of the Server Management Services is described more fully in the Responsibility chart below and include the following:

- recovery of hardware fault incident management and correction of fault condition; and
- Server hardware preventative maintenance.

Server Hardware Fault Management	Province	Service Provider
Service Provider will detect, escalate, resolve, and perform root cause analysis (as described in Services Management SOW) for all Server hardware faults on both the Province Owned Equipment and the Service Provider Owned Equipment.		R
To the extent possible Service Provider will perform Server maintenance during scheduled Maintenance Windows, and in all cases in accordance with the Change Management Process described in the Services Management SOW.		R
Service Provider will perform emergency Server maintenance as determined by Service Provider, and in all cases in accordance with the Change Management Process described in the Services Management SOW.		R

At the request of the Province (EHS) Service Provider will not undertake any non-critical Changes on specified Servers during the period requested by the Province ("**Change Freeze**"). Service Provider may undertake critical Changes on such specified Servers during the Change Freeze in accordance with the Change Management Process described in the Services Management SOW		R
Service Provider will perform preventative maintenance on the hardware, to the extent necessary and as determined by the Service Provider, to achieve the Service Levels relating to the operation and performance of the Servers under this SOW. Service Provider will perform any changes required as a result of such preventive maintenance services in accordance with the Change Management Process.		R

1.4.9 Operating System Support and Fault Management

The Operating System Support and Fault Management component of the Server Management Services describes the Operating System ongoing support to detect, escalate, resolve and perform root cause analysis (as described in the Services Management SOW) and preventive maintenance on Images as may be necessary for Service Provider to achieve all applicable Service Levels. The Operating System Support and Fault Management component of the Server Management Services is described more fully in the Responsibility chart below and includes the following:

- management, administration and tuning of Operating Systems;
- backup of Operating System and non-user file systems;
- updates to configuration elements as provided by Province;
- recovery of Image Fault; and
- Image preventive maintenance.

Operating System Support and Fault Management	Province	Service Provider
The Service Provider will adjust the Operating System parameters to improve performance of the associated Client Applications and the Server to extent technically possible (tuning).		R

Operating System Support and Fault Management	Province	Service Provider
The Service Provider will provide restore capabilities for non-user file systems, Operating Systems, related tools and Client Applications related files that are local to the Operating System partition, with a recovery point objective of the previous business day and working with Client as required. Service Provider will restore to the most current recovery point technically possible.		R
The Service Provider will establish a backup schedule that minimizes impact to Province and Client operations and meets a previous business day recovery point objective.		R
When the Service Provider makes changes to the Operating System functionality that could adversely impact the Client's Applications, then the Service Provider will make such changes in accordance with the Change Management Process.		R
Service Provider will determine, to the extent that it is able to, whether such changes to the Operating System functionality could adversely impact Client's Applications.		R
Service Provider will interact as necessary with third-party Operating System and other system-level software product suppliers for Operating System and other system-level software support.		R
Province will provide Service Provider with updates to configuration elements as required for Service Provider to perform ongoing support under this SOW: • Server name • Associated Province directory services systems • User IDs • User Security Access • Storage partition information • Internet Protocol address information • Required information to align with Security SOW	R	

Operating System Support and Fault Management	Province	Service Provider
• File system security settings		
The Service Provider will review Operating System product status and maintenance information to identify current related trends and potential problems with the Operating Systems in use under this SOW, and provide the Province "Thought Leadership" seminars at least annually.		R
The Service Provider will perform preventive maintenance to Operating System to prevent known problems to Operating System, in accordance with the Change Management Process.		R
The Service Provider will maintain (and update as required) Operating System configuration documentation.		R
Service Provider will provide file system management, such as: • Create, maintain, modify and delete volumes and directory structures • Verify mount point availability • Adjust file system sizes and top level permissions • Repair defective file systems		R
The Service Provider will monitor the up/down status of the Server, as required and determined by Service Provider to achieve the applicable Service Levels.		R
Recovery from Image Fault and correct the Fault condition through Incident and Problem Management Process described in the Services Management SOW.		R
Permit installation of the Image monitoring software agents and tools, subject to the requirements of the Security SOW, to allow Service Provider to monitor the Image.	R	
Service Provider will install Image monitoring software agents and tools, subject to the requirements of the Security SOW, to allow Service Provider to monitor the Servers.		R

Operating System Support and Fault Management	Province	Service Provider
Service Provider will perform preventive maintenance on the Server, to the extent necessary and as determined by the Service Provider, and perform any changes resulting from the preventive maintenance in accordance with the Change Management Process.		R
Service Provider will monitor and manage Operating System related logs as may be required for Service Provider to perform preventive maintenance and fault resolution related to the Operating Systems and Servers.		R
Service Provider will assist the Client with the creation of Application logs within the Operating System in accordance with the Change Management Process.		R
Service Provider will perform recovery for file system, directory, or individual file as requested by Clients in accordance with the Change Management Process.		R

1.4.10 Patch Management

The Patch Management component of the Server Management Services describes Service Provider's responsibility for monitoring and planning for, and applying, patches to the Operating Systems and the Service Provider installed monitoring and tracking tools, based upon the Change Management Process described in the Services Management SOW. The Patch Management component of the Server Management Services is described more fully in the Responsibility chart below.

Patch Management	Province	Service Provider
Monitor relevant third-party suppliers and industry bulletins for Operating System security-related patch alerts.		R
The Service Provider will plan and apply patches for Service Provider supported software (being Operating Systems and Service Provider installed software tools) in accordance with the Change Management Process and where applicable the Security SOW. Where the Clients do not provide the necessary consent under the Change Management Process for any required patches to be		R

applied, then on an exception basis Service Provider will request the Province (EHS) to either resolve the matter or provide the necessary consent.		
Service Provider will apply patches as requested by the Province and Clients from time to time following the procedures set forth in the Midrange Operating Manual and the Change Management Process.		R
Clients, at their discretion, to provide necessary testing of Clients' business Applications following any Service Provider supported software patch installation.	R	

1.4.11 Server Hardware Upgrading and Replacement

The Server Hardware Upgrading and Replacement component of the Server Management Services describes Service Provider's responsibility to maintain contact with applicable hardware vendors to maintain Service Provider's knowledge of current offerings and support issues, and to replace both Province Owned Equipment and Service Provider Owned Equipment based upon Service Provider's obligations under the Agreement as well as may be required for Service Provider to achieve applicable Service Levels. The selection of Server Hardware upon replacement is addressed in Appendix J (*Server Technology Evolution*). The Server hardware Upgrading and Replacement component of the Server Management Services is described more fully in the Responsibility chart below.

Server Hardware Upgrading and Replacement	Province	Service Provider
Service Provider will review hardware and hardware maintenance information to identify current related trends and potential problems with the hardware in use.		R
Service Provider will replace the hardware at the hardware's end of life as required under the Agreement, taking into account the "virtual" transformation project contemplated under the Transformation SOW.		R
Service Provider will install, verify functionality and remove hardware components as required to meet vendor recommendations or Client requirements, in accordance with the Change Management Process.		R

1.4.12 Server Operating System Upgrading

The Server Operating System Upgrading component of the Server Management Services describes Service Provider's responsibility to monitor, track and recommend (and where approved in accordance with this SOW install) Operating System upgrades based upon software currency requirements as specified under the Agreement and Supporting SOWs, and as may otherwise be required to maintain vendor support of the Operating System. The Server Operating System Upgrading component of the Server Management Services is described more fully in the Responsibility chart below and in Appendix I (*Major Midrange Software Release Upgrades*).

As part of the Annual Planning process the Parties will review Operating System currency for all Operating Systems in use in the Supported Infrastructure. For Operating Systems that will no longer be supported in the next 12 months by Operating System vendors, the Service Provider will inform the Province and Clients. Should the Client wish to remain on an unsupported version of the Operating System, as approved by the Province (EHS), the Service Provider will notify the Client and Province of any changes to the services in relation to that unsupported Operating System and any associated risks.

Server Operating System Upgrading	Province	Service Provider
Service Provider will recommend Operating System upgrades to Clients as required to maintain vendor support of the Operating System.		R
Service Provider will install Operating System upgrades, in accordance with the Change Management Process, to maintain currency as required for Client Applications and as specified by the "Technology Improvement and Currency" portion of the Annual Operating Plan.		R
Clients, at their discretion, to provide necessary testing of Clients' business Applications following any Service Provider supported Operating System upgrade.	R	

1.4.13 Regular and Ongoing Client Interaction

The Regular and Ongoing Client Interaction component of the Server Management Services describes Service Provider's responsibility to maintain ongoing Province and Client interactions with respect to Server Management Services Requests and to work with the Province and the Clients, as applicable, to resolve application issues that may be related to Server hardware, firmware or Operating Systems. Service Provider will answer questions from Province and Client personnel with respect to Server hardware, firmware and Operating Systems. The Regular and Ongoing Client Interaction component of the Server Management Services is described more fully in the Responsibility chart below.

Regular and Ongoing Client Interaction	Province	Service Provider
Service Provider will answer questions regarding Servers and Operating Systems from the Province and Clients related to the Server Management Services under this SOW.		R
Service Provider will meet with Clients from time to time at the reasonable request of the Client on a scheduled or ad hoc basis to discuss future plans, current issues, upcoming technological changes, project related work and other similar matters.		R
Service Provider will work with Clients to resolve business Application issues that may be related to the Servers or Operating Systems.		R
Service Provider will perform administrative Operating System activities for Clients who do not have sufficient Operating System privileges to support the Clients' business Applications, as required (such as stopping or starting services, running batch jobs, running scripts, file system related activities).		R

1.4.14 Remote Server Support

The Remote Server Support component of the Server Management Services describes the ability of the Service Provider to remotely provide the Server Management Services to the Province Midrange Facilities. The Remote Server Support component of the Server Management Services is described more fully in the Responsibility chart below.

To the extent that the Server Management Services to be provided by Service Provider at the Province Midrange Facilities are dependent on the Province fulfilling its obligations under the Agreement (including those described in the Responsibility chart below), and the Province fails to perform such obligations, then the Service Provider will be relieved of its obligations to the extent of such dependency and until such time as the Province performs its obligations (and for greater clarification the Province may continue its non-performance for such period of time as the Province may determine).

Remote Server Support	Province	Service Provider
To the extent possible the Service Provider will provide the Server Management Services under this SOW to the Province Midrange Facilities remotely through the Province's shared network (SPAN/BC), and otherwise provide the Server Management Services at the Province's Facilities in accordance		R

Remote Server Support	Province	Service Provider
the On-Site SOW.		
Province will provide Service Provider with access, through the Province's shared network (SPAN/BC) and in accordance with the Security SOW, to the Servers in the Province Midrange Facilities that are subject to the Server Management Services, and that are connected to Province's shared network (SPAN/BC).	R	
Service Provider to provide the Province with such information as may be required by the Province to provide Service Provider with access to Servers through the Province shared network (SPAN/BC)		R
Province to provide a secure physical area at all Province Midrange Facilities for Servers supported by the Service Provider.	R	

1.4.15 Image Performance Management Services

The Image Performance Management Services component of the Server Management Services monitors and reports on the performance of the Image's components on both physical and virtual Servers. Service Provider will commence the Image Performance Management Services following the installation of the Service Provider management tools in the first six months following the Hand-Over Date. The Image Performance Management Services is described more fully in the Responsibility chart below.

Image Performance Management Services	Province	Service Provider
Service Provider will monitor Image components (such as CPU percent utilization, File system percent used, Memory utilization, Image Availability) using Service Provider's monitoring tools and provide monthly performance reports on a per Image basis as set forth in Appendix B.		R
Service Provider will set the monitoring agents to the Service Provider's standard monitoring thresholds. The Service Provider will adjust these thresholds as required by the Province and agreed to by the Service Provider acting reasonably.		R

1.4.16 Server and Equipment Decommission

The Server and Equipment Decommission component of the Server Management Services describes Service Provider's responsibility to decommission Province Owned Equipment and Service Provider Owned Equipment, including removal and disposal, in accordance with the Change Management Process, the security requirements of the Security SOW, and the STMS Data Centre SOW. The Server and Equipment Decommission component of the Server Management Services is described more fully in the Responsibility chart below.

Server and Equipment Decommission	Province	Service Provider
Service Provider will decommission Province Owned Equipment and Service Provider Owned Equipment in accordance with the Change Management Process and as is more particularly described in the Midrange Operating Manual.		R
Service Provider will archive Server security logs for decommissioned Servers in accordance with the Security SOW.		R
Service Provider will update the systems for which Service Provider has responsibility (such as backup scheduling systems, monitoring systems), to reflect the removal of the decommissioned Servers, as per the Midrange Operating Manual.		R
Province will update the systems for which Province has responsibility to reflect the removal of the decommissioned Servers (such as the Province Active Directory, network ACLs).	R	
Service Provider will disconnect the decommissioned Province Owned Equipment and Service Provider Owned Equipment from all connections (such as power, network, storage) in Province Midrange Facilities.		R
Service Provider will notify the Province that the Province Owned Equipment and Service Provider Owned Equipment (as applicable) is decommissioned.		R
Service Provider will update Service Provider's asset management system for Service Provider Owned Equipment.		R

Service Provider will remove and deliver all decommissioned Province Owned Equipment and Service Provider Owned Equipment in accordance with the requirements of the Security SOW, Province Security Policies & Standards and the Province's "IT Asset Disposal" process (which "IT Asset Disposal" process is more fully described in the Midrange Operating Manual).		R
The Province will provide Service Provider all necessary training and access to paperwork relating to the removal and delivery of Province Owned Equipment.	R	
Service Provider will complete all necessary paperwork relating to the removal and delivery of Province Owned Equipment, and will provide copies of all such paperwork (paper copies or electronic copies) to the Province (EHS) at the time of completion or such other time as the Parties may agree.		R
Province will destroy or recycle Province Owned Equipment, as applicable, in accordance with the Security SOW.	R	
Service Provider will destroy or recycle Service Provider Owned Equipment, as applicable, in accordance with the Security SOW.		R
Service Provider will maintain cleanliness and tidiness of Service Provider areas of Province Midrange Facilities		R

S. 15

S. 15

S. 15

1.4.18 Image Performance Management – Optional Services

Image Performance Management – Optional Services provides Image performance reports, analysis and performance recommendations and implementation based upon the use of Operating System statistics (such as CPU, Memory and File System space). These services may be purchased for the minimum period set forth in the Schedule 23 of the Agreement, or longer.

Image Performance Management – Optional Services	Province	Service Provider
Service Provider will configure the Service Provider's management tools installed on the Servers to obtain Optional Image performance data and performance trends as requested by the Client through Province Ordering System (such as resource usage statistics indicators like CPU, memory, input/output (I/O), and storage).		R

Image Performance Management – Optional Services	Province	Service Provider
On a monthly basis, Service Provider will analyze and report to the Client regarding the Image performance data and performance trends.		R
To the extent possible and feasible, the Client will provide Service Provider with forecasted volume growth (such as the volume of data or the number of users) that may impact Image performance.	R	
Based upon the monthly analysis and reports, Service Provider will make recommendations to the Client to improve Image performance.		R
Service Provider will review the Image performance recommendations with the Clients.		R
Service Provider will consult with the Clients to determine which Image performance recommendations, if any, should be implemented.		R
Service Provider will implement recommendations approved by the Client through the Change Management Process.		R

1.4.19 Server Capacity – Optional

Server Capacity – Optional analyzes historical Server resource usage (such as CPU, memory, and storage trends) for a maximum of 12 prior months on a rolling basis. This analysis is then used to forecast Server resource usage and compares the historical Server usage to the Server's existing resources. This service is available for physical and virtual Servers.

Server Capacity – Optional	Province	Service Provider
On a monthly basis, Service Provider will analyze the Server resource usage (such as CPU, memory and storage) for the previous 12 month period, and provide the Client with a report indicating the Server resource usage trends.		R
To the extent possible and feasible, the Client will provide Service Provider with forecasted volume growth (such as the volume of data or the number of users) that may impact Server resource usage.	R	

Server Capacity – Optional	Province	Service Provider
Based upon the monthly analysis and reports, Service Provider will make recommendations to the Client to prevent the Client from running out of available Server resources (such as CPU, Memory and storage).		R
Where requested by the Client, Service Provider will review the Server resource usage recommendations with the Client.		R
Consult with the Clients to determine which Server resource usage recommendations, if any, should be implemented.		R
Service Provider will implement recommendations approved by the Client through the Change Management Process.		R

1.4.20 Cluster Management - Optional

The Cluster Management – Optional services of the Server Management Services describes Service Provider's responsibility to provide a High Availability (HA) Server layer by configuring and clustering Servers together. This service is delivered though the installation and maintenance of system software and related tools, as well as database and application software that is required to provide an HA Server configuration environment. The Cluster Management Services – Optional component of the Server Management Services is described more fully in the Responsibility chart below.

Cluster Management - Optional	Province	Service Provider
Clients will work with the Service Provider to specify the Server requirements for clustering, such as: • Number of nodes • Servers to be used • Server location • Application requirements	R	
Service Provider will design cluster configuration required to meet the Clients specifications and Server requirements.		R

Cluster Management – Optional	Province	Service Provider
Client will review and approve Service Provider cluster configuration proposed by Service Provider.	R	
Client will request necessary hardware and clustering services following the Province Ordering System Process.	R	
Service Provider will install, configure, test and maintain the hardware and software required to support the approved Server cluster configuration.		R
Client will install Client Applications on the Server cluster.	R	
Client will conduct tests to determine whether the Client's Applications on the Server cluster fail-over correctly, and if the testing requires the production servers, then promotion of the Client's Application will be through the Change Management Process.	R	
Service Provider will assist the Client, upon request, in conducting tests to determine whether the Client's Applications on the Server cluster fail-over correctly.		R
Service Provider will plan, perform, document and report to the Client on annual fail-over tests to validate the Server cluster's Operating System fail-over functionality. Fail-over testing will be through the Change Management Process.		R
Service Provider will determine, through root cause analysis, if the cause for Server unavailability is due to the Server Operating System Libraries (such as Dynamic Link Libraries on Window Servers) being altered by the Clients.		R

1.4.21 Application Monitoring Services – Optional

The Application Monitoring Services – Optional component of the Server Management Services describes Service Provider's responsibility to provide operational support to monitor Province and Client Application alerts, and is based upon the availability of Service Provider monitoring agents for the Applications in question. The Application Monitoring Services – Optional component of the Server Management Services is described more fully in the Responsibility chart below.

Application Monitoring Services – Optional	Province	Service Provider
Service Provider will provide monitoring agents for Client Application software as available from the Service Provider's monitoring infrastructure (such as monitoring agents, monitor Servers, monitoring consoles and so on).		R
Clients will define Application monitoring requirements such as monitoring counters and thresholds requiring monitoring.	R	
Service Provider will install monitoring agents on Client requested Servers		R
Service Provider will configure monitoring agents as determined by the Client's Application monitoring requirements.		R
Service Provider will escalate detected events through the Incident Management process defined in the Services Management SOW.		R

1.4.22 Batch Management Services – Optional

The Batch Management Services – Optional component of the Server Management Services describes Service Provider's responsibility to provide batch job scheduling and batch job monitoring for Province's and Client's Application hosted on the Supported Infrastructure. The batch job scheduling involves the activities associated with defining and maintaining an Application's batch processing within the Service Provider's scheduling system. The batch job monitoring involves the activities associated with monitoring the execution functions of an Application's batch processing that is scheduled to run. If abnormal job termination occurs for the batch job, Service Provider will execute predefined instructions and processes to either restart the job or escalate the issue to the Province or the Client, as applicable. The Batch Management Services – Optional component of the Server Management Services is described more fully in the Responsibility chart below.

Batch Management Services – Optional	Province	Service Provider
Client will define scheduling requirements (such as triggers, dependencies, start conditions, restart instructions) for Client specific batch jobs ("Supported Batch Jobs").	R	

Batch Management Services – Optional	Province	Service Provider
Service Provider will install, configure, maintain, operate, and remove as necessary Service Provider standard batch scheduling software in accordance to the Change Management Process defined in the Services Management SOW.		R
Service Provider will create and schedule, test and validate Supported Batch Jobs and provide test results to Clients.		R
Client will review Supported Batch Job test results to confirm whether the Supported Batch Job meets Client requirements or not.	R	
The Client in consultation and working with the Service Provider will determine reason for the Supported Batch Job failure and resolve cooperatively.	R	
Service Provider will consult and work with the Client as the Client resolves the Supported Batch Job failure.		R
Create automated Supported Batch Job completion alerts for the Client and deliver by email as required by the Client.		R
Client will provide Service Provider with any changes to the Supported Batch Jobs and any changes required for the Supported Batch Job schedule.	R	
Service Provider will maintain Supported Batch Job schedules and operational support of the scheduling system.		R
Service Provider will assist the Client in performing Supported Batch Job scheduling and related problem determination and resolution.		R
Service Provider will monitor for batch execution (Supported Batch Job started) of all Supported Batch Jobs.		R
Service Provider will notify the Client of any failed batch execution (Supported Batch Job started) of all Supported Batch Jobs.		R

Batch Management Services – Optional	Province	Service Provider
Service Provider will resolve the failed batch execution (Supported Batch Job started) of all Supported Batch Jobs where the cause of the failure is due to the Service Provider's Batch Job Scheduling software.		R
Clients, at their discretion, will resolve the failed batch execution (Supported Batch Job started) of a Supported Batch Job where the cause of the failure is due to other than the Service Provider's Batch Job Scheduling software.	R	

APPENDIX A DEFINED TERMS / DEFINITIONS

Defined Term	Definition
7 x 24	24 hours per day, 7 days per week and allows for Planned Downtime scheduled through the Change Management Process.
Application	Software that provides functions that are required by a Client in support business processes (but excludes the Operating System and Server firmware).
Application Monitoring Services – Optional	Means the services described in Section 1.4.21 of this SOW.
Architecture	The conceptual design and fundamental operational structure of a computing system.
Client	Client Ministries or the WTS, as applicable.
Central Processing Unit (CPU)	A machine that can execute computer programs.
Domain Name Service (DNS)	A service that provides the mapping of a Server name and its internet protocol address in any given computer network.
S. 15	
Fault	An operational event that differs sufficiently from the expected norm and that generally warrants some specific corrective action be taken in response.
Image	An instance of an Operating System and related software (e.g. anti-virus, monitoring software, and such) running on a physical or Virtual Server.
Image Availability	The measure of time that an Image is operating and accessible in a networking environment (such as for purposes of making Server resources to Applications).
Incident	Has the meaning given to it in the Services Management SOW.
Least Privileged Access	The least amount Elevated privileges as are necessary for the Clients to maintain their Applications or perform the tasks required of them.

Defined Term	Definition
Maintenance Window	An assigned and approved period of time for performing maintenance to Servers (such as hardware, Operating System and software preventive and corrective procedures).
Operating System	The infrastructure software component of a computer system responsible for the management and coordination of activities and the sharing of the resources of the computer.
Privileged Accounts	A user with allocated rights within the computing environment which are greater than those available to the majority of other users and include systems administrators, network administrators and database administrators. Responsibilities include keeping the systems available, and may include rights to create new users profiles, or change the privileges and access rights of existing users or take action which may affect computing systems, network communication, or the accounts, files, data, or processes or other users.
Province (EHS)	Enterprise Hosting Solutions branch of the Ministry of Labour & Citizens' Services of the Province of British Columbia, or its successor.
Province Data Centres	Data centres managed by the Province at premises owned or leased by the Province as listed in Schedule 8 (*Service Locations*) of the Agreement.
Province Midrange Facilities	The Province Data Centres, the Regional Network Centres and the Remote Sites
Province Licenses	Province software license held by the Province for which Use Rights are granted to the Service Provider
Province Owned Equipment	The Supported Infrastructure as of the Hand-Over Date and includes any hardware that is added to the Supported Infrastructure after the Hand-Over Date which is owned by the Province.
Province Service Delivery Groups	The organizational entities within the Province responsible for certain services within the Province.
Regional Network Centres	Equipment rooms managed by the Province at premises owned or leased by the Province as listed in Schedule 8 (*Service Locations*) of the Agreement, as amended by the Province through the Change Management Process or the Change Order Process as applicable.

Defined Term	Definition
Remote Sites	A site that houses a one or more Servers at premises owned or leased by the Province as listed in Schedule 8 (*Service Locations*) of the Agreement, as amended by the Province through the Change Management Process or the Change Order Process as applicable.
Server	A physical or virtual instance of computer hardware.
Service Provider Owned Equipment	The components of the Supported Infrastructure owned by the Service Provider.
Service Provider Tools	Servers and software provided by the Service Provider for use in the management and delivery of Services and excludes Supported Infrastructure (such as monitoring Servers and software, automation Servers and software, patch management Servers and software, network management Servers and software, storage management Servers and software, backup management Servers and software) .
Space License Agreement	The License Agreement dated March 30, 2009 between the Province and the Service Provider for the use of certain space by the Service Provider at S. 15
STMS Data Centres	The STMS Calgary Data Centre and the STMS Interior Data Centre (each as defined in the Data Centre SOW).
Virtual Server	An instance of a Server that maintains the appearance and capabilities of the Operating System without being associated with physical hardware
Windows Domain Level Privileged Accounts	Accounts that have privileged access to Active Directory domains, such as Domain Admins.

APPENDIX B MIDRANGE REPORTS

1. Availability By Resource Report

The following reports will be based upon the Servers for each Client, except for the Service Provider's tool Servers.

This report shows the system availability, outage duration and counts, actual uptime based on SNMP uptime with unscheduled outages listed and overall availability percentage calculated. Includes fields to show unscheduled downtime (outages) and expected uptime. The detail section shows the outage details such as the start time, end time and outage duration.

1.1 Availability By Resource Report (Summary Page)

Availability By Resource

Report Period: 2006-07-01 - 2006-12-31

Color Legend	
Critical	
Warning	
Target	
Optimum	

Client Name Appears Here

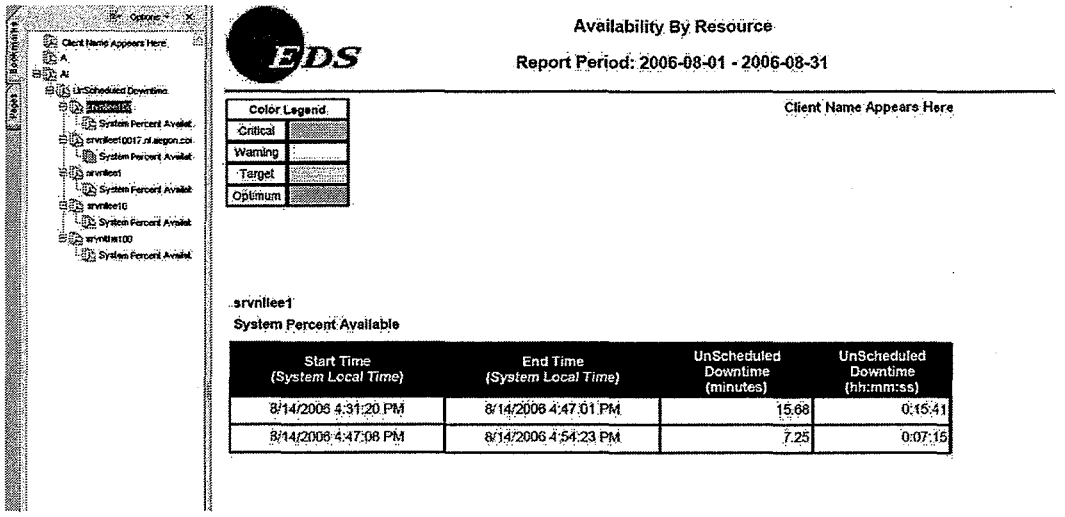
ABC

System Percent Available

system	UnScheduled Downtime	Expected Uptime	Total Uptime	Percent Availability	Number of Outages	Scheduled Downtime	Scheduled Minutes
USDLS7ERSQ02	15	41711.43	41696.43	99.964%	1	0	0
USPLD7ERDC04	0	10728.92	10728.92	100%	0	0	0
USPLS7ERDAF2	0	224.8	224.8	100%	0	0	0
USPLS7ESRWD1	0	20880	20880	100%	0	0	834.1
USPLS7ESSWD1	0	807.25	807.25	100%	0	0	0
USPLS7ETDEV2	0	222.72	222.72	100%	0	0	0
USPLT7EVVTS1	0	20291.42	20291.42	100%	0	0	0
USPLV7ETHV01	0	525.8	525.8	100%	0	0	0
Total	15	95182.13	95177.13	99.9955%	1	0	834.1

- Frequency: Monthly
- Recipient: Province

1.2 Availability By Resource Report (Detail Page)



Availability By Resource

Report Period: 2006-08-01 - 2006-08-31

Color Legend
Critical
Warning
Target
Optimum

Client Name Appears Here

srvnllee1

System Percent Available

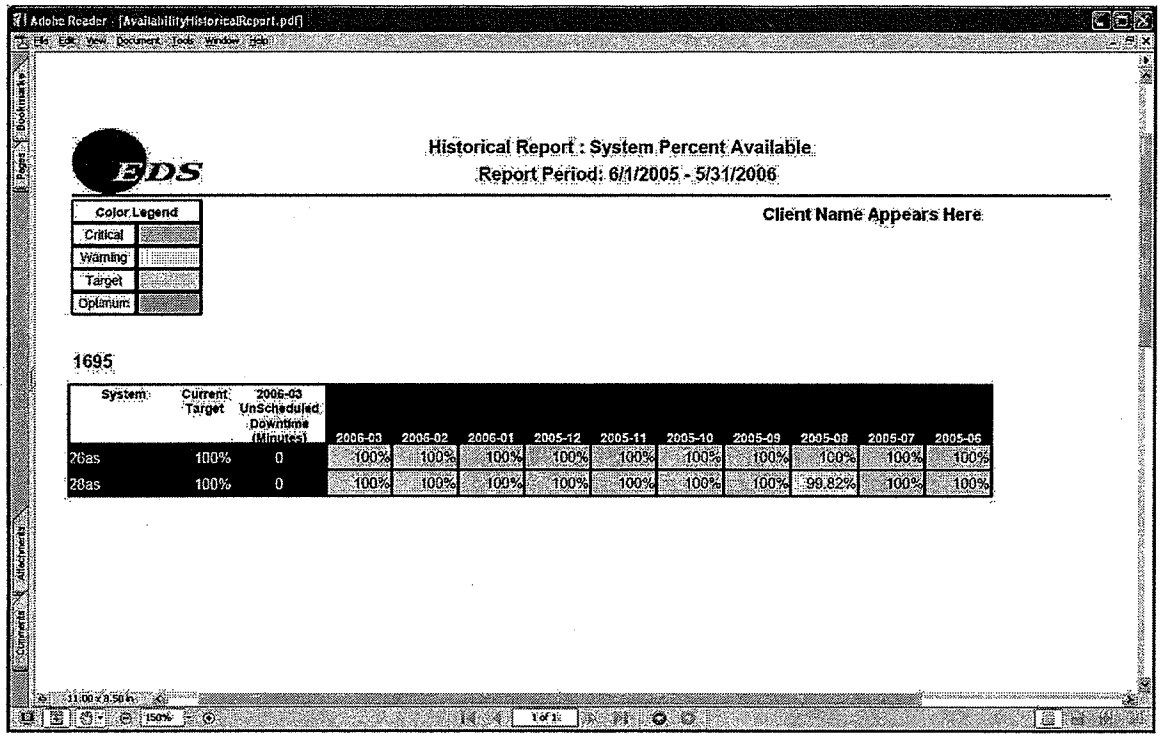
Start Time (System Local Time)	End Time (System Local Time)	UnScheduled Downtime (minutes)	UnScheduled Downtime (hh:mm:ss)
8/14/2006 4:31:20 PM	8/14/2006 4:47:01 PM	15.68	0:15:41
8/14/2006 4:47:08 PM	8/14/2006 4:54:23 PM	7.25	0:07:15

- Frequency: Monthly
- Recipient: Province

2. Availability Historical Report

This report shows the historical availability per resource for the report period. Includes fields to show current target and downtime minutes for the latest months.

2.1 Availability Historical Report



Historical Report : System Percent Available
Report Period: 6/1/2005 - 5/31/2006

Client Name Appears Here

Color Legend	
Critical	
Warning	
Target	
Optimum	

1695

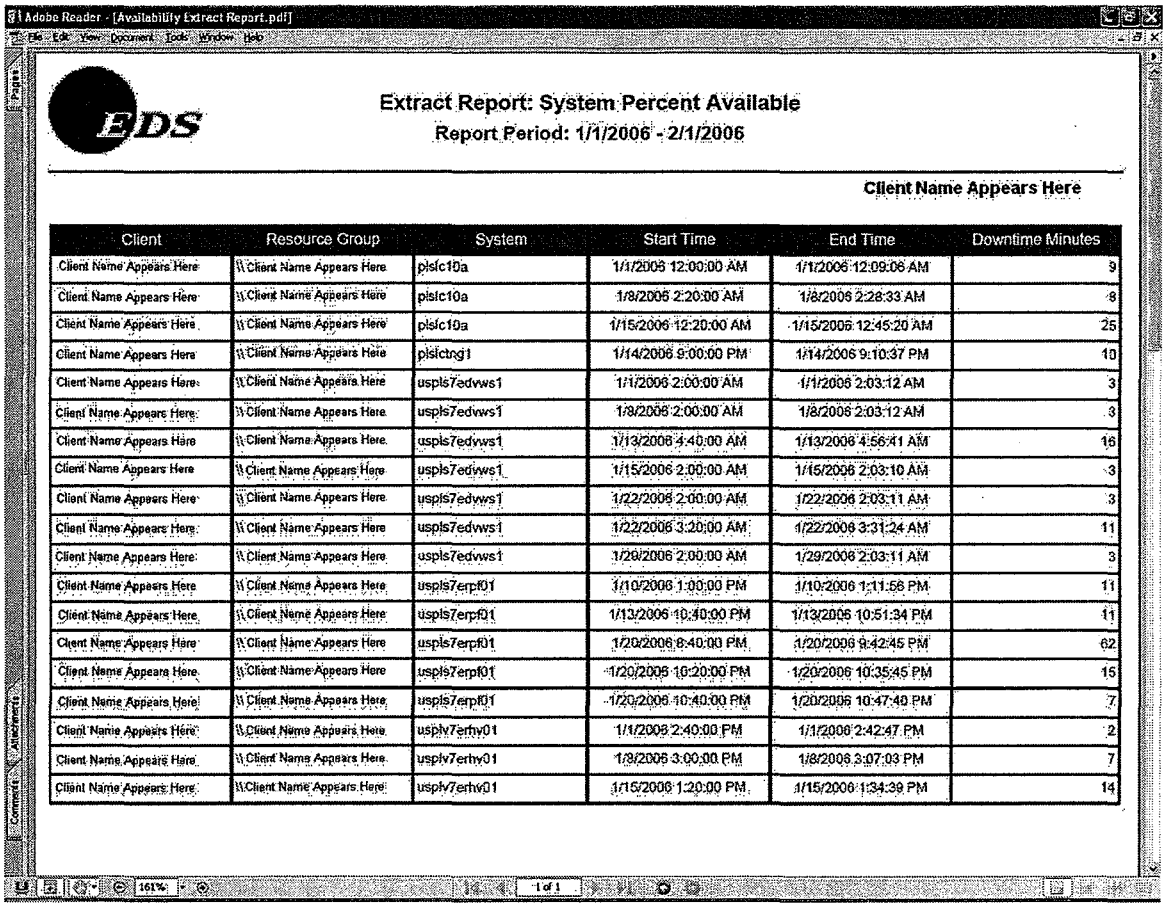
System	Current Target	2006-03 UnScheduled Downtime (Minutes)	2006-03	2006-02	2006-01	2005-12	2005-11	2005-10	2005-09	2005-08	2005-07	2005-06
26as	100%	0	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
28as	100%	0	100%	100%	100%	100%	100%	100%	100%	99.82%	100%	100%

- Frequency: Monthly
- Recipient: Province

3. Availability Extract Report

The monthly excel extract shows the downtime minutes listed per host

3.1 Availability Extract Report



Extract Report: System Percent Available
Report Period: 1/1/2006 - 2/1/2006

Client Name Appears Here

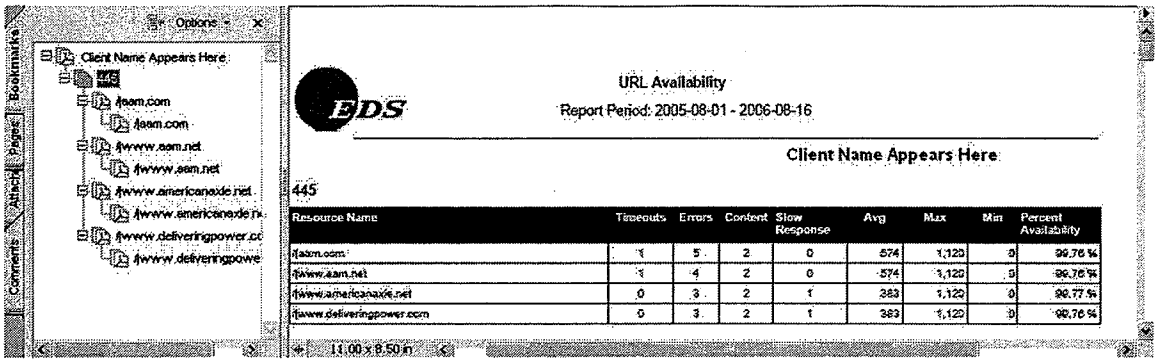
Client	Resource Group	System	Start Time	End Time	Downtime Minutes
Client Name Appears Here	\\Client Name Appears Here	plslc10a	1/1/2006 12:00:00 AM	1/1/2006 12:09:06 AM	9
Client Name Appears Here	\\Client Name Appears Here	plslc10a	1/8/2006 2:20:00 AM	1/8/2006 2:28:33 AM	8
Client Name Appears Here	\\Client Name Appears Here	plslc10a	1/15/2006 12:20:00 AM	1/15/2006 12:45:20 AM	25
Client Name Appears Here	\\Client Name Appears Here	plslctxg1	1/14/2006 9:00:00 PM	1/14/2006 9:10:37 PM	10
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/1/2006 2:00:00 AM	1/1/2006 2:03:12 AM	3
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/8/2006 2:00:00 AM	1/8/2006 2:03:12 AM	3
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/13/2006 4:40:00 AM	1/13/2006 4:56:41 AM	16
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/15/2006 2:00:00 AM	1/15/2006 2:03:10 AM	3
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/22/2006 2:00:00 AM	1/22/2006 2:03:11 AM	3
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/22/2006 3:20:00 AM	1/22/2006 3:31:24 AM	11
Client Name Appears Here	\\Client Name Appears Here	uspls7edvws1	1/29/2006 2:00:00 AM	1/29/2006 2:03:11 AM	3
Client Name Appears Here	\\Client Name Appears Here	uspls7erpf01	1/10/2006 1:00:00 PM	1/10/2006 1:11:56 PM	11
Client Name Appears Here	\\Client Name Appears Here	uspls7erpf01	1/13/2006 10:40:00 PM	1/13/2006 10:51:34 PM	11
Client Name Appears Here	\\Client Name Appears Here	uspls7erpf01	1/20/2006 8:40:00 PM	1/20/2006 9:42:45 PM	62
Client Name Appears Here	\\Client Name Appears Here	uspls7erpf01	1/20/2006 10:20:00 PM	1/20/2006 10:35:45 PM	15
Client Name Appears Here	\\Client Name Appears Here	uspls7erpf01	1/20/2006 10:40:00 PM	1/20/2006 10:47:40 PM	7
Client Name Appears Here	\\Client Name Appears Here	usplv7erhv01	1/1/2006 2:40:00 PM	1/1/2006 2:42:47 PM	2
Client Name Appears Here	\\Client Name Appears Here	usplv7erhv01	1/8/2006 3:00:00 PM	1/8/2006 3:07:03 PM	7
Client Name Appears Here	\\Client Name Appears Here	usplv7erhv01	1/15/2006 1:20:00 PM	1/15/2006 1:34:39 PM	14

- Frequency: Monthly
- Recipient: Province

4. URL Availability Report

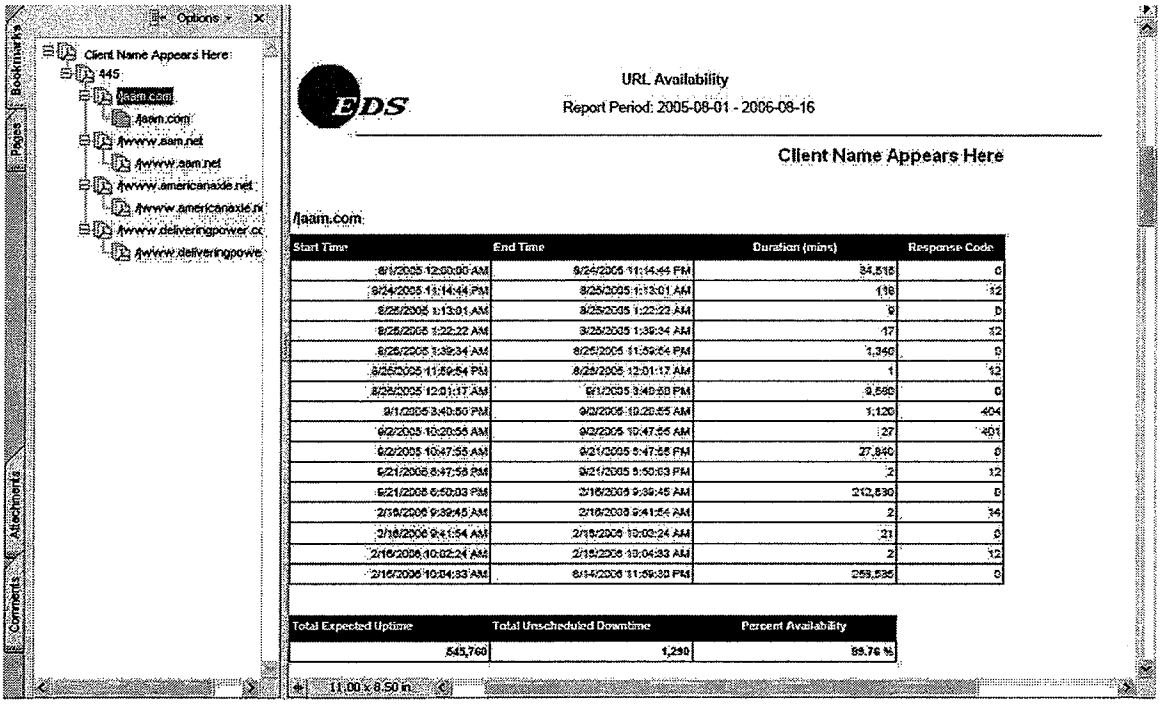
This report shows the URL Availability summary and detail. The summary section (above) includes fields to show the total number of timeouts, errors, content, slow responses and percent availability. The detail section (below) shows the outage detail per incident. For websites, availability reporting as specified in the Web Hosting Services SOW.

4.1 URL Availability Report (Summary Page)



Resource Name	Timeouts	Errors	Content	Slow Response	Avg	Max	Min	Percent Availability
/aam.com	1	5	2	0	574	1,120	0	99.76 %
/www.aam.net	1	4	2	0	574	1,120	0	99.76 %
/www.americanaxle.net	0	3	2	1	383	1,120	0	99.77 %
/www.deliveringpower.com	0	3	2	1	383	1,120	0	99.76 %

4.2 URL Availability Report (Detail Page)



Start Time	End Time	Duration (mins)	Response Code
8/1/2005 12:00:00 AM	8/24/2005 11:14:44 PM	34,515	0
8/24/2005 11:14:44 PM	8/25/2005 1:13:01 AM	118	12
8/25/2005 1:13:01 AM	8/25/2005 1:22:22 AM	9	0
8/25/2005 1:22:22 AM	8/25/2005 1:39:34 AM	17	12
8/25/2005 1:39:34 AM	8/25/2005 11:59:54 PM	1,340	0
8/25/2005 11:59:54 PM	8/25/2005 12:01:17 AM	1	12
8/25/2005 12:01:17 AM	9/1/2005 3:40:50 PM	9,580	0
9/1/2005 3:40:50 PM	9/2/2005 10:20:55 AM	1,120	404
9/2/2005 10:20:55 AM	9/2/2005 10:47:55 AM	27	401
9/2/2005 10:47:55 AM	9/21/2005 5:47:58 PM	27,840	0
9/21/2005 5:47:58 PM	9/21/2005 5:50:03 PM	2	12
9/21/2005 5:50:03 PM	2/16/2006 9:39:45 AM	212,630	0
2/16/2006 9:39:45 AM	2/16/2006 9:41:54 AM	2	14
2/16/2006 9:41:54 AM	2/16/2006 10:03:24 AM	21	0
2/16/2006 10:03:24 AM	2/16/2006 10:04:33 AM	2	12
2/16/2006 10:04:33 AM	8/14/2006 11:59:30 PM	259,535	0

Total Expected Uptime	Total Unscheduled Downtime	Percent Availability
545,760	1,290	99.76 %

- Frequency: Monthly
- Recipient: Province

5. Capacity Reporting (Base)

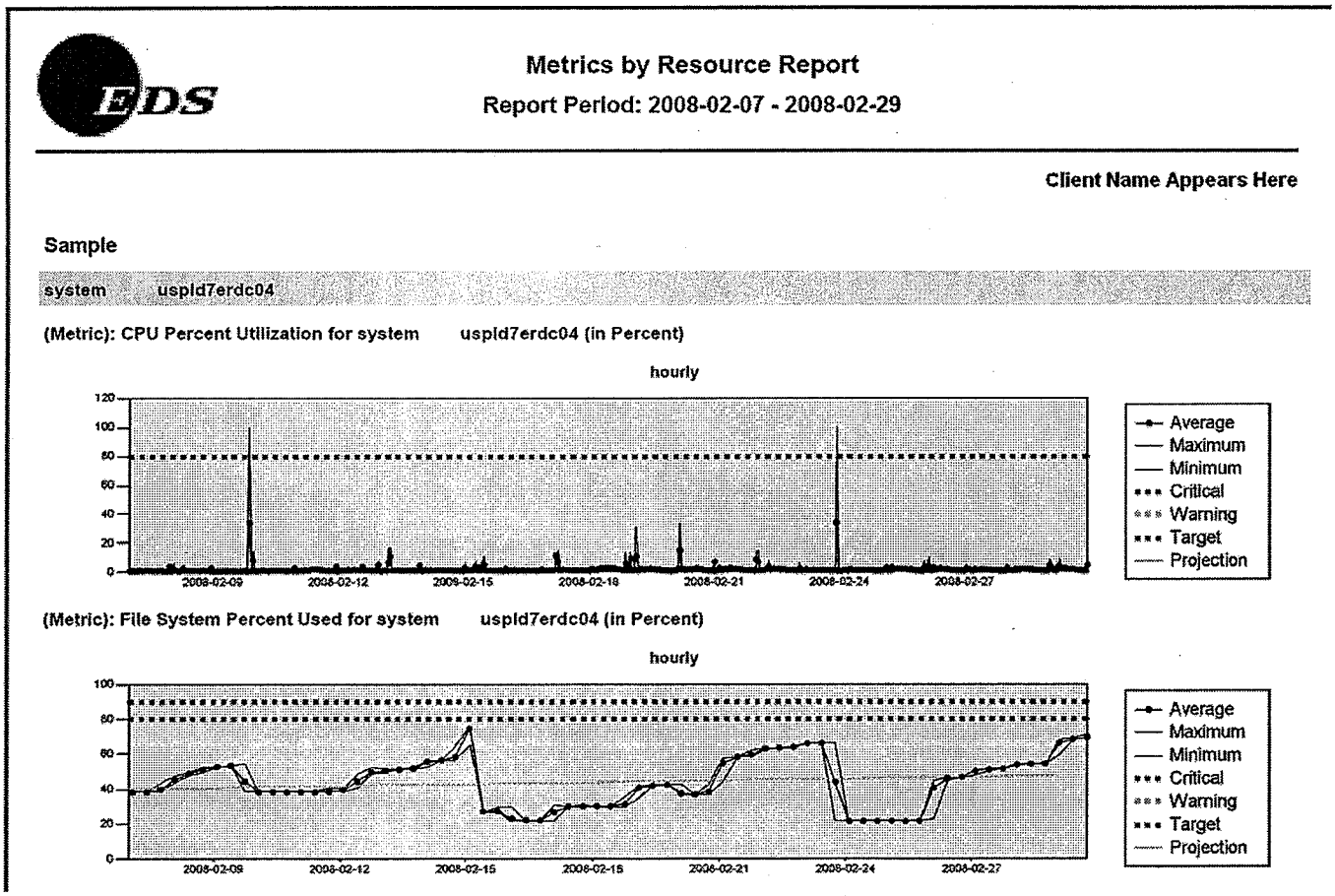
Base set of reports that allow for an understanding of the current Server resource usage, related to Capacity.

6. Metrics By Resource Report

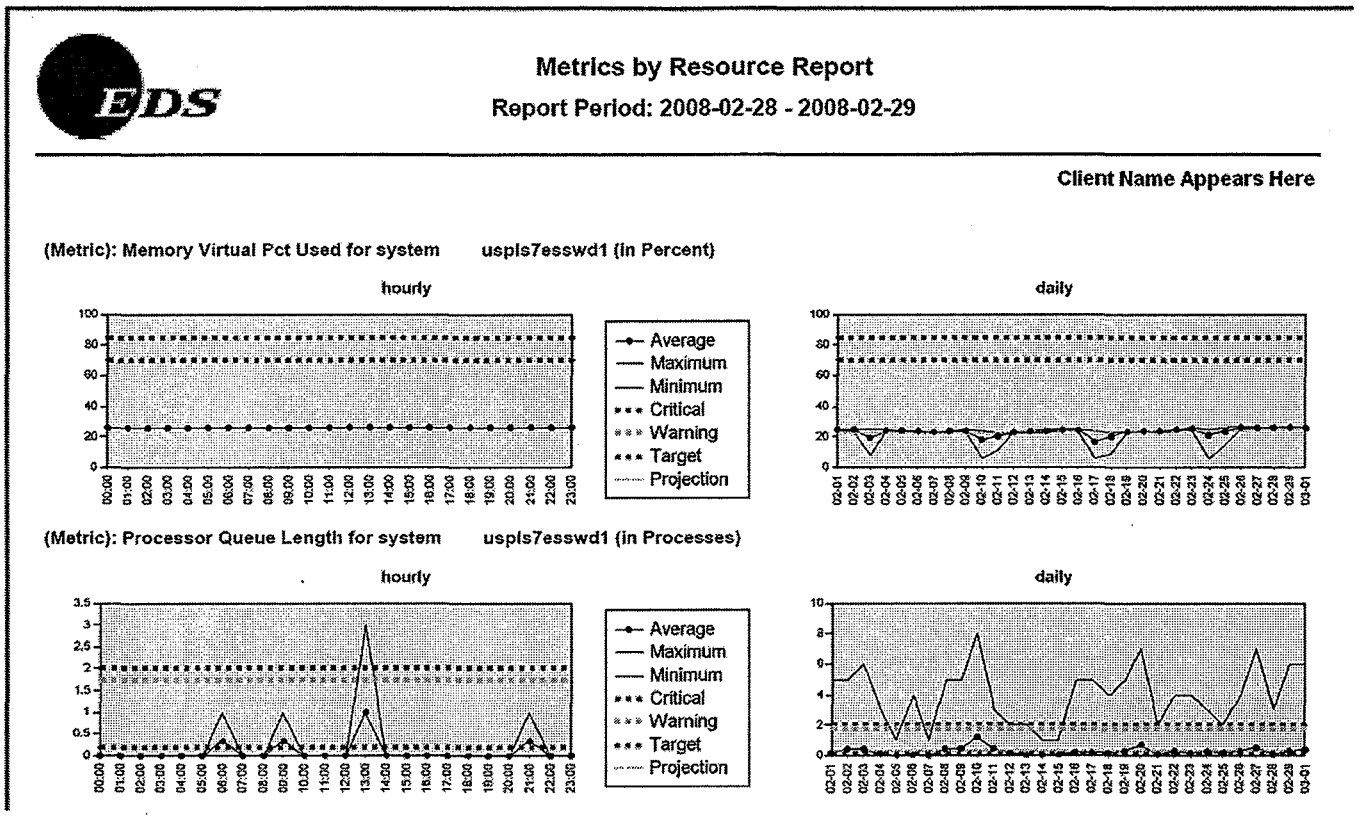
This report graphically presents any (specified) non-availability metric data by 1 or 2 selected optional intervals (hourly, daily, weekly, monthly) and corresponding interval date ranges for the specified resource-types. These options are set at the time the report is created. Report can include:

- min/max/avg data with threshold values for each resource/metric.
- Ability to project and chart values into future.
- Ability to independently control interval and date-range of left/right graphs thru parameters.
- 1-Up option for wider graphs. 2-Up option for side-by-side graphs.

6.1 Metrics by Resource Report (1-Up option)



6.2 Metrics by Resource Report (2-Up option)



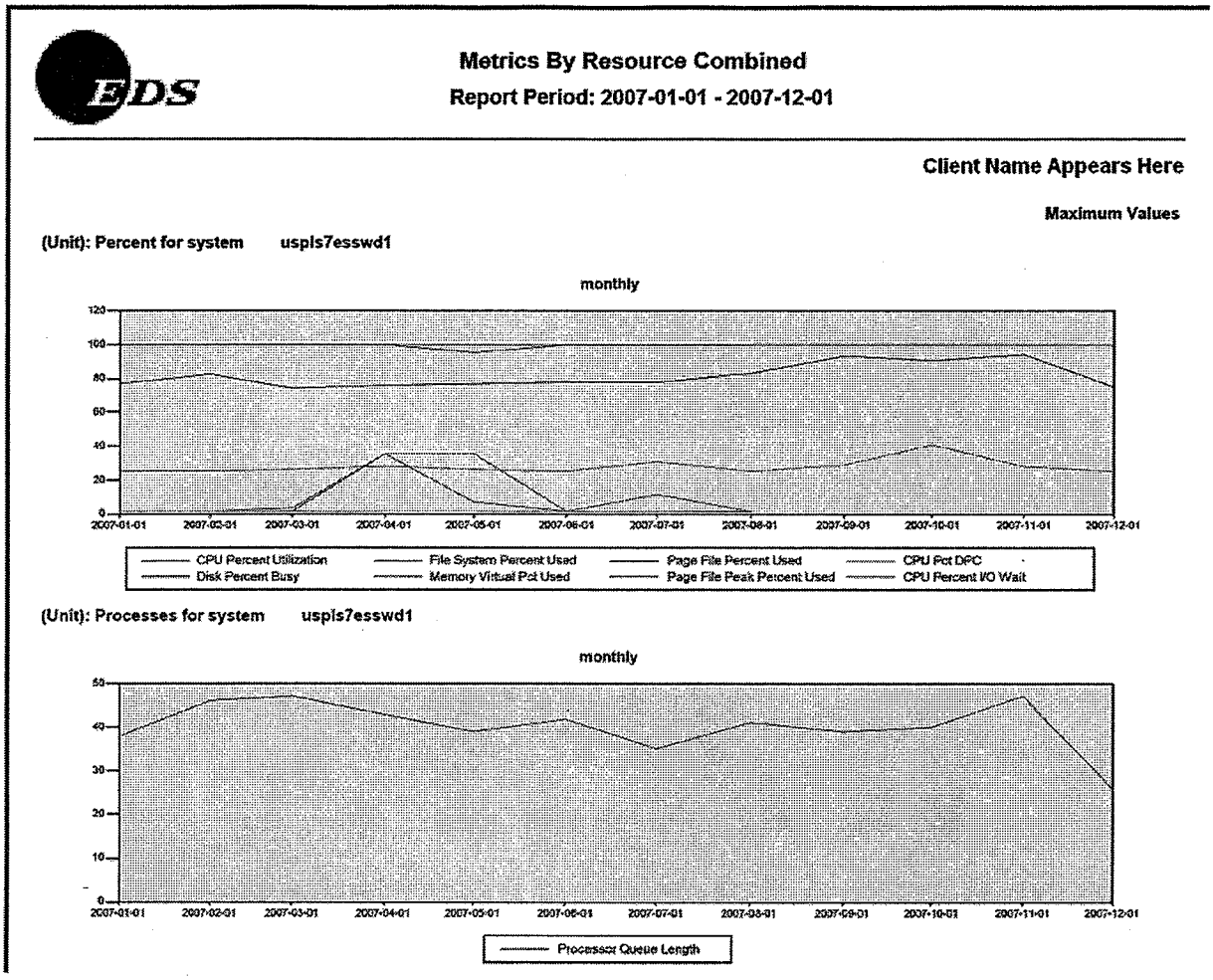
- Frequency: Monthly
- Recipient: Province

7. Metrics By Resource Combined Report

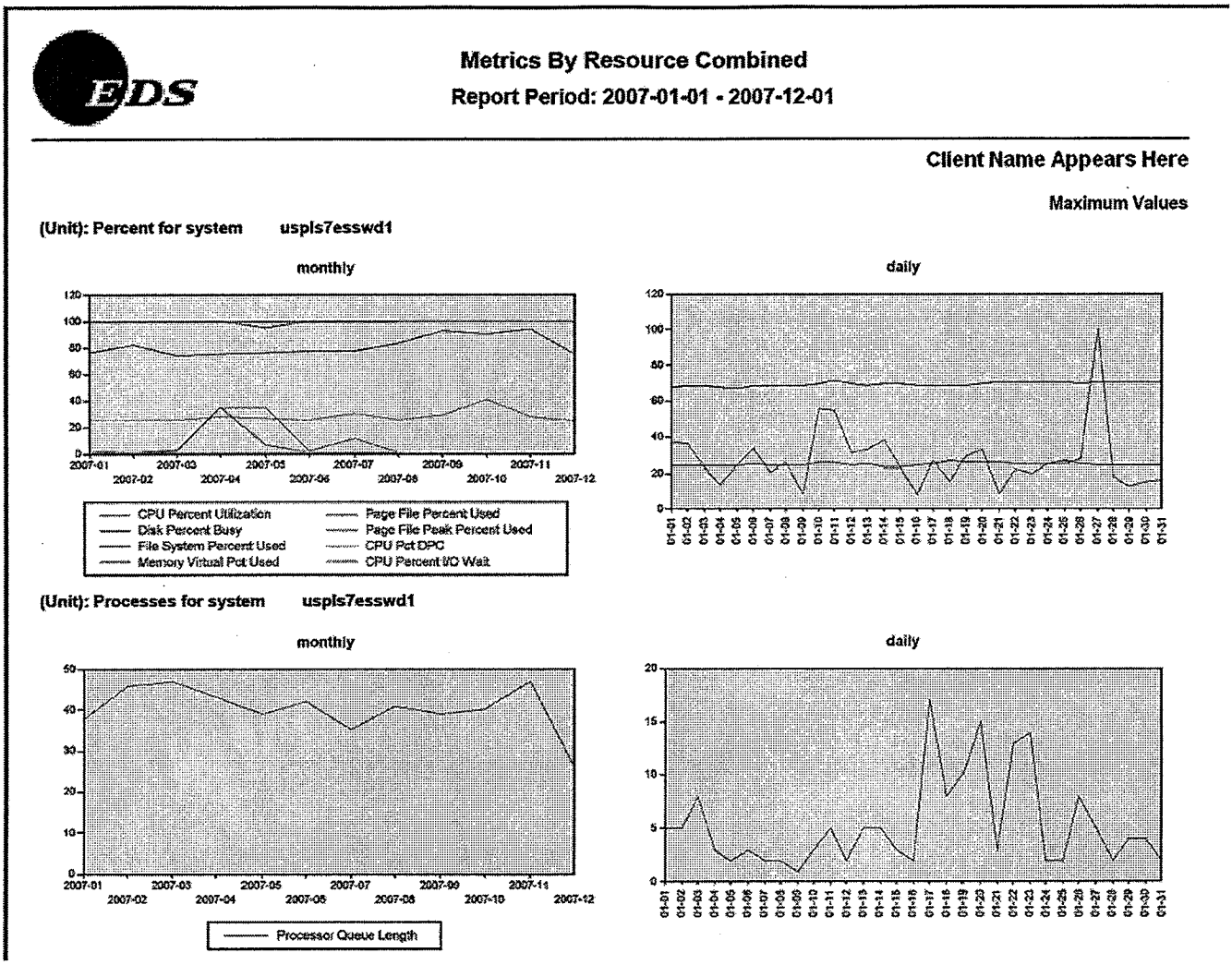
This report graphically presents specified non-availability metric data by 1 or 2 optional intervals (hourly, daily, weekly, monthly) and corresponding interval date ranges for the resources specified resource-types. These options are set at the time the report is created. Report may include:

- Intervals and date-ranges on left and right graphs are controlled independently.
- Output combines metrics for resources according to their units of measure into a single graph.
- Aggregation of values (min, max, avg) to display is parameter driven.
- 1-Up option for wider graphs. 2-Up option for side-by-side graphs.

7.1 Metrics by Resource Combined Report (1-Up option)



7.2 Metrics by Resource Combined Report (2-Up option)



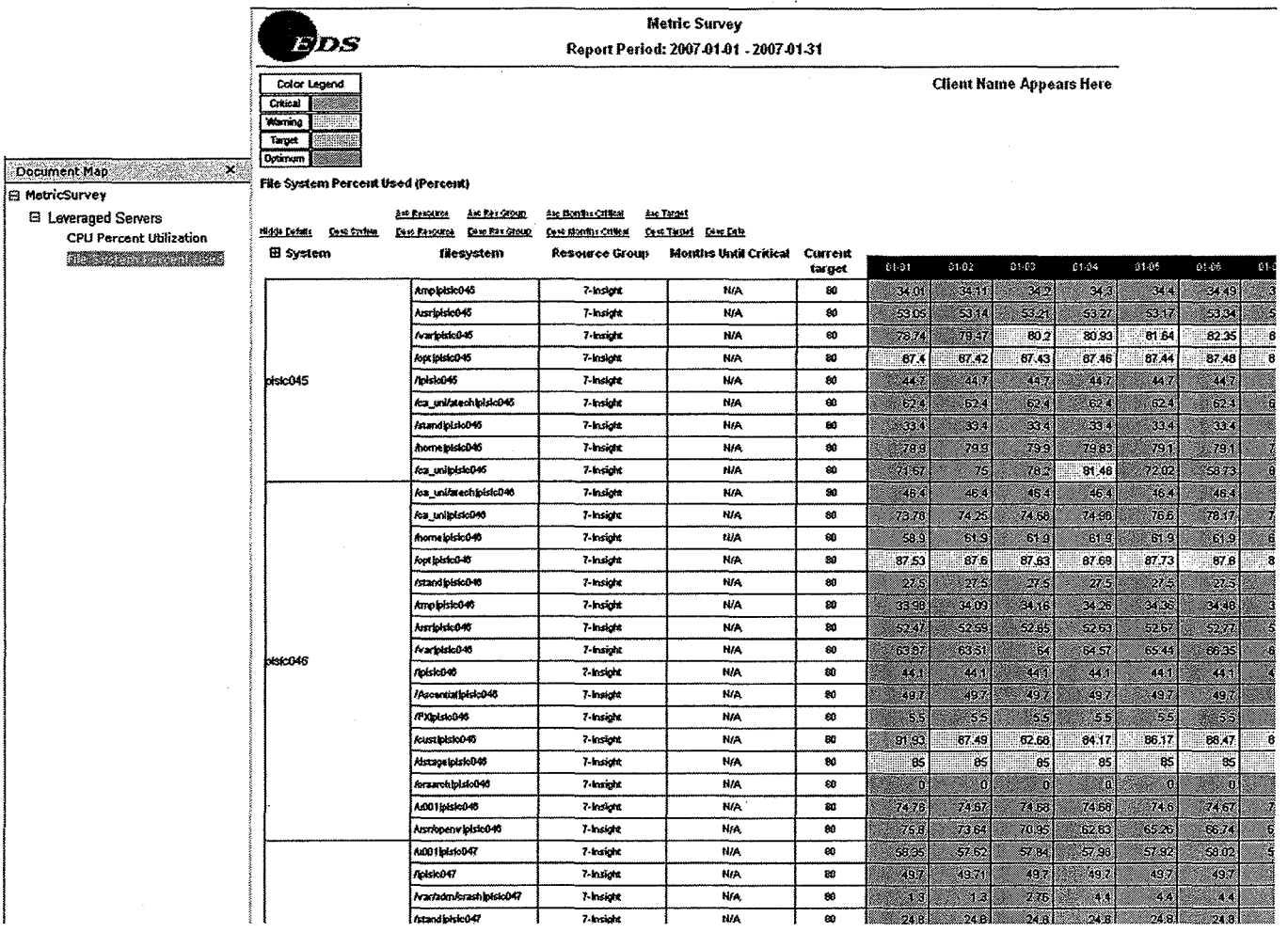
- Frequency: Monthly
- Recipient: Province

8. Metric Survey Report

This report displays a grid containing aggregated metric values for each resource by a user-selected interval (hourly, daily, weekly, monthly) for the report period. Resources and their children are grouped together. Report may include:

- Ability to project values into future and color-shade projections based on thresholds
- Exception run options
- Schedulable options include sorting of rows and columns

8.1 Metric Survey Report



Metric Survey

Report Period: 2007-01-01 - 2007-01-31

Client Name Appears Here

Color Legend: Critical, Warning, Target, Optimum

Document Map

- MetricSurvey
  - Leveraged Servers
    - CPU Percent Utilization

File System Percent Used (Percent)

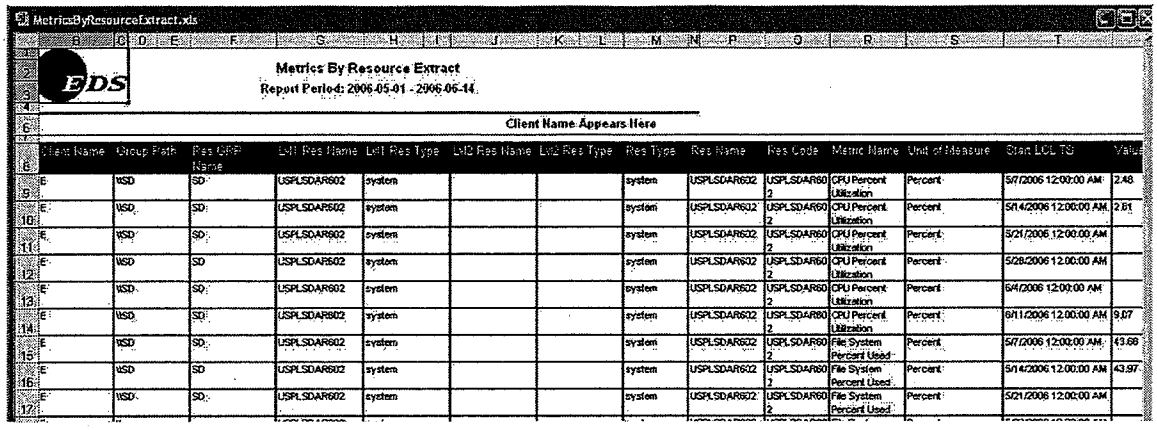
System	Filesystem	Resource Group	Months Until Critical	Current target	01-01	01-02	01-03	01-04	01-05	01-06	01-
plsic045	/tmp\plsic045	7-Insight	N/A	80	34.01	34.11	34.2	34.3	34.4	34.49	3
	/usr\plsic045	7-Insight	N/A	80	53.05	53.14	53.21	53.27	53.17	53.04	5
	/var\plsic045	7-Insight	N/A	80	78.74	79.47	80.2	80.93	81.64	82.35	8
	/opt\plsic045	7-Insight	N/A	80	87.4	87.42	87.43	87.46	87.44	87.48	8
	/\plsic045	7-Insight	N/A	80	44.7	44.7	44.7	44.7	44.7	44.7	
	/ca_uni/atech\plsic045	7-Insight	N/A	80	62.4	62.4	62.4	62.4	62.4	62.4	6
	/stand\plsic045	7-Insight	N/A	80	33.4	33.4	33.4	33.4	33.4	33.4	
	/home\plsic045	7-Insight	N/A	80	78.9	79.9	79.9	79.83	79.1	79.1	7
	/ca_uni\plsic045	7-Insight	N/A	80	71.67	75	78.2	81.46	72.02	58.73	6
plsic046	/ca_uni/atech\plsic046	7-Insight	N/A	80	46.4	46.4	46.4	46.4	46.4	46.4	
	/ca_uni\plsic046	7-Insight	N/A	80	73.78	74.25	74.68	74.96	76.6	76.17	7
	/home\plsic046	7-Insight	N/A	80	58.9	61.9	61.9	61.9	61.9	61.9	6
	/opt\plsic046	7-Insight	N/A	80	87.53	87.6	87.63	87.69	87.73	87.8	8
	/stand\plsic046	7-Insight	N/A	80	27.5	27.5	27.5	27.5	27.5	27.5	
	/tmp\plsic046	7-Insight	N/A	80	33.98	34.09	34.16	34.26	34.36	34.48	3
	/usr\plsic046	7-Insight	N/A	80	52.47	52.59	52.65	52.53	52.57	52.77	5
	/var\plsic046	7-Insight	N/A	80	63.87	63.51	64	64.57	65.44	66.35	6
	/\plsic046	7-Insight	N/A	80	44.1	44.1	44.1	44.1	44.1	44.1	4
	/Accential\plsic046	7-Insight	N/A	80	49.7	49.7	49.7	49.7	49.7	49.7	
	/PX\plsic046	7-Insight	N/A	80	5.5	5.5	5.5	5.5	5.5	5.5	
	/cust\plsic046	7-Insight	N/A	80	91.93	67.49	62.68	84.17	86.17	88.47	8
	/stage\plsic046	7-Insight	N/A	80	85	85	85	85	85	85	
	/research\plsic046	7-Insight	N/A	80	0	0	0	0	0	0	
	/u001\plsic046	7-Insight	N/A	80	74.79	74.67	74.68	74.68	74.6	74.67	7
	/usr/openv\plsic046	7-Insight	N/A	80	75.8	73.64	70.95	62.63	65.26	66.74	6
	/u001\plsic047	7-Insight	N/A	80	58.95	57.62	57.84	57.96	57.92	58.02	5
	/\plsic047	7-Insight	N/A	80	49.7	49.71	49.7	49.7	49.7	49.7	
	/var/adm/crash\plsic047	7-Insight	N/A	80	1.3	1.3	2.76	4.4	4.4	4.4	
	/stand\plsic047	7-Insight	N/A	80	24.8	24.8	24.8	24.8	24.8	24.8	

- Frequency: Monthly
- Recipient: Province

9. Metrics By Resource Extract Report

Results include unformatted, detailed output data for capacity metrics, including: metric data, thresholds, projections, and ratings. Can be exported as a continuous csv file or excel file.

9.1 Metrics By Resource Extract Report



MetricsByResourceExtract.xls

EDS

Metrics By Resource Extract
Report Period: 2006-05-01 - 2006-06-14

Client Name Appears Here

Client Name	Group Path	Res QRF Name	Lvl1 Res Name	Lvl1 Res Type	Lvl2 Res Name	Lvl2 Res Type	Res Type	Res Name	Res Code	Metric Name	Unit of Measure	Start LCL TS	Value
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	CPU Percent Utilization	Percent	5/7/2006 12:00:00 AM	2.48
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	CPU Percent Utilization	Percent	5/14/2006 12:00:00 AM	2.61
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	CPU Percent Utilization	Percent	5/21/2006 12:00:00 AM	
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	CPU Percent Utilization	Percent	5/28/2006 12:00:00 AM	
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	CPU Percent Utilization	Percent	6/4/2006 12:00:00 AM	
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	CPU Percent Utilization	Percent	6/11/2006 12:00:00 AM	9.07
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	File System Percent Used	Percent	5/7/2006 12:00:00 AM	43.68
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	File System Percent Used	Percent	5/14/2006 12:00:00 AM	43.97
E	\SD	SD	USPLSDAR602	system			system	USPLSDAR602	USPLSDAR602	File System Percent Used	Percent	5/21/2006 12:00:00 AM	

- Frequency: Monthly
- Recipient: Province
- Capacity Reporting: Optional

APPENDIX C SYSTEMS

Intentionally Left Blank

APPENDIX D SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

APPENDIX F SUPPORTED OPERATING SYSTEMS

Service Provider will provide Midrange Services for the Windows, OpenVMS, Solaris, Linux and AIX Operating Systems on Hand-Over Date.

The Province has identified that the Servers to be supported by the Service Provider as part of the Managed Services include the HPUX and Tru64 Servers. From and after the Hand-Over Date:

(i) the Service Provider will use commercially reasonable efforts to provide the Midrange Services for the HPUX and Tru64 Servers in accordance with the Agreement; and

(ii) if the Service Provider's management tools and agents cannot be used on the HPUX or Tru64 Servers, then the matter will be addressed through the Change Order Process.

APPENDIX G MANAGED SERVICES – STORAGE OF SURPLUS PHYSICAL SERVER HARDWARE

The Province has the ability to increase and decrease the number of physical Servers that reside in a data centre and are subject to the Server Management Services. When a decrease in the number of physical Servers occurs and the physical Server has remaining asset life (as described in Schedule 23 of the Agreement), then the physical Server will be added to an inventory of available physical Servers ready for deployment, referred to as "**Available Inventory**".

The Available Inventory will remain in the Server rack in which it was previously installed and will be powered off and "wipe" the disks. The Service Provider will use Province standard procedures to wipe internal hard drives of the Available Inventory in accordance with the Province's IT Asset Disposal which is listed Schedule 28 of the Agreement. When the Service Provider receives a request (or where there is otherwise a requirement) to deploy a new physical Server, the Service Provider will first consider redeploying physical Servers of the same type from the Available Inventory before purchasing a new physical Server. The Service Provider will recommend to the Province which physical Server from the Available Inventory should be deployed instead of purchasing a new physical Server (based upon the requirements giving rise to the need for a new Server), subject to the approval of the Province, and for greater clarification, the Province will either:

(a) accept the Service Provider's recommendation to use a particular physical Server from the Available Inventory;

(b) select another Server of the same type from the Available Inventory to use instead of the particular Server recommended by the Service Provider; or

(c) determine not to use a Server from the Available Inventory, in which case, the Service Provider will dispose of the Server so recommended to the Province in order to prevent a build up of inventory in the rack space, and will notify the Province of such disposal.

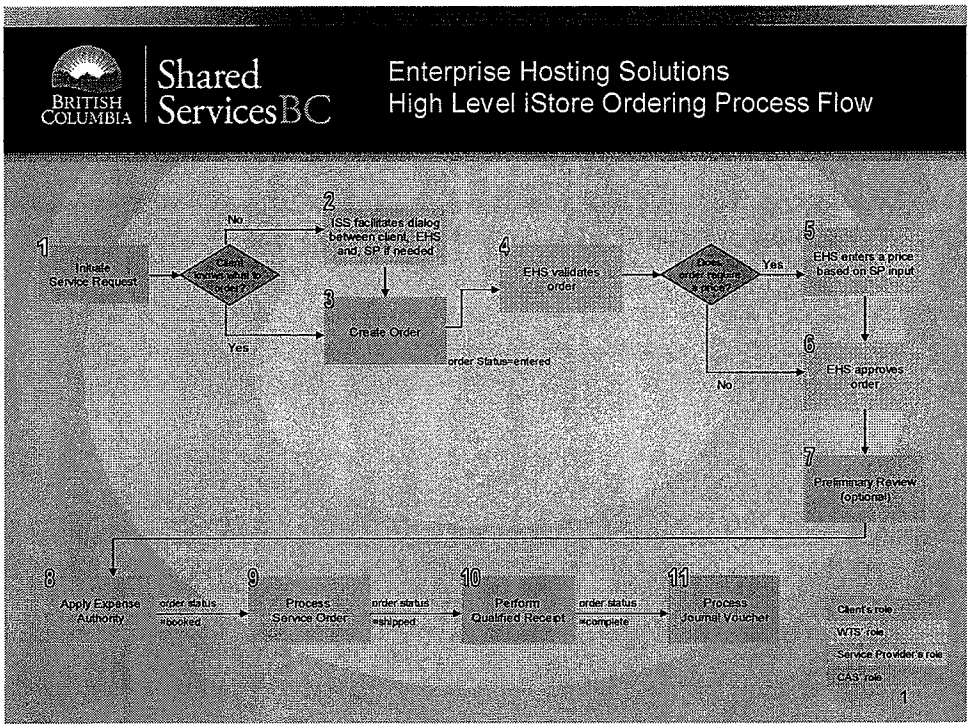
The Service Provider will dispose of any Server in the Available Inventory that has passed its end of life, being a period of 5 years per Server.

The Parties expect that the racks in the STMS Data Centre will not be full and will have capacity to hold the Available Inventory. Should the Available Inventory exceed the available rack space in the Server Provider Data Centre, then the Service Provider will inform the Province and the Parties will work together to determine a suitable solution which may include any of the following (and if they are unable to agree upon a suitable solution, then the matter will be resolved through Governance):

(a) disposing of some of the Available Inventory, or

(b) pursuant to a Change Order, moving the Available Inventory to an agreed offsite storage location.

APPENDIX H MANAGED SERVICES – PROVINCE ORDERING SYSTEM PROCESS FLOW



APPENDIX I MAJOR MIDRANGE SOFTWARE RELEASE UPGRADES

1. Major software releases includes new release and major version updates of OS, database, web, Citrix and middleware software.

2. It is the goal of the Parties to maintain technology at sufficient levels of currency to support interoperability amongst software products required by the Province and to enable the ability for the Province to take advantage of enhanced functionality wherever required within the Province's enterprise technology.

3. Service Provider will make new major software releases available for deployment as part of its Gold Build package. This will happen when the product is stable (usually about 12 months after software vendor General Availability) and upon completion of certification to test for stability and interoperability with OS', systems management and monitoring tools provided by Service Provider.

4. As part of its service, Service Provider will identify, test and document applicable new features that may be inherent in a new major software release, identifying the potential benefit and impact of those features to the Province. The activation and deployment of any new software feature may be subject to a Change Order should the feature be deemed to require a material effort to activate and deploy or should it be deemed to have a material impact to the underlying costs of the Services.

5. For new or refreshed systems:

    a. The most current Gold Build versions of software will be used unless the Client requires continued use of a prior version of the software (likely for Application compatibility reasons)

    b. If the Client requires that the prior version of software be retained, the Province (EHS) will approve the request for the Client to retain the prior version of the software. While that software continues to be vendor supported, Service Provider will fully support with Service Levels.

    c. If the software is no longer vendor supported, Service Provider will support but without Service Levels using resources providing service to the STMS project. If the software introduces security risks, then Service Provider and the Province will need to agree on how such security risks are dealt with.

6. For in-place systems:

    a. Once a system has been refreshed as part of the Transformation project, if Service Provider supplied software required for Managed Services goes out of software vendor support, Service Provider will take responsibility for the Service Provider effort to upgrade the software on the in-place systems unless a Client had previously chosen and received Province approval to remain on an older version

of software at the time of the prior refresh. In this case Service Provider will have the right to a Change Order associated with the in place upgrade. Should a client require the retention of the unsupported version of software, Service Provider will support but without Service Levels using available resources. If the software introduces security risks, then Service Provider and the Province will need to agree on how such security risks are dealt with.

b. For Shared Services (SFP, Citrix, virtual hosts etc.):

i. Service Provider will determine whether in-place upgrades are required to achieve compliance to the software vendor's maintenance requirements and, in conjunction with the Province, the required functionality of the Shared Service. If required, Service Provider will undertake those upgrades as part of the service.

ii. The Province will perform all required testing and any necessary Application changes to ensure that Province and Client Applications and services dependant on the Shared Services are compliant to such upgrades.

c. For all other systems:

i. If a Client requires a software upgrade prior to its scheduled refresh, the Client may request Service Provider to provide an early refresh of the system involved. Service Provider recommends that this be performed as a migration from the Client's existing server(s) to a "new" server(s) for the Client. For physical and virtual Servers there are two methods to achieve this type of migration;

1. For physical Servers, the early refresh of physical server may utilize the process for Surplus Servers as described in the Server Management Services SOW and Fee Schedule.

2. For Virtual Servers, the Client is only required to commit to three months of usage of any Virtual Server. Additional Virtual Servers can be made available to the Client with the upgraded software, as available in the Service Provider Gold Build. Once the client has migrated to the "new" Virtual Servers as required by the Client, and three or more months of service has been consumed on the "old" Virtual Servers, the Client may decommission the old Virtual Servers.

ii. If a Client requires an in-place upgrade of software on any single or clustered server prior the server's planned refresh, Service Provider will have the right to a Change Order.

APPENDIX J SERVER TECHNOLOGY EVOLUTION

This document deals with the baseline hardware architecture for Servers that the Service Provider will be implementing as of the Effective Date. The Service Provider will, as requested through the Province Ordering System or through the Service Provider service commitments, install the hardware models with the noted server performance ratings and power consumption

As this hardware and the Operating Systems age, product vendors will declare these products as reaching end of life at which time vendor product support will terminate. To provide the ongoing identification of new products of a similar performance and capacity, the Service Provider has utilized the HP Product Quick Reference Guide that rates Wintel based hardware using a SPECint rating system and the SUN "M" rating system for SUN Solaris products. This will facilitate the identification of products having similar capacities in the evolution of the hardware that the Service Provider will supply in satisfying Province requirements. The power consumption ratings of Servers has also been provided as one of the overall objectives of the Service Provider and the Province is to satisfy the Province demand for hosting services while achieving power consumption reductions through the use of more power efficient hardware.

Software currency and the alternatives for introducing new versions of software are addressed in this SOW (1.4.12 Server Operating System Upgrading and Appendix I major midrange software release upgrades).

Initial Service Provider STMS Server Models

Sun x86 Servers		SPECint_rate2006	Power Rating (W) at 80 % Average Utilization
Web Server	Sun X4140 server with 1 AMD quad core processor, 4GB Memory kit (2x 2GB), 2x73GB disks, 2 PSUs	45	207
Base Server	Sun X4140 server with 2 AMD quad core processors, 8GB Memory (2x4GB), 2x146GB disks, 2 PSUs	87	263
VMware Backup Server	Sun X4240 server with 2 AMD quad core processors, 8GB Memory, 2x146GB disks, 2 PSUs	87	281
App/DB Server	Sun X4240 server with 2 AMD quad core processors, 16GB Memory, 2x146GB disks, 2x4GB HBAs, 2 PSUs	87	298
VMware Server	Sun X4440 server with 2 AMD quad core processors, 64GB Memory (16x4GB), 3x146GB disks, 2x4GB HBAs, 2 PSUs	87	423

Sun Unix Servers		M-Value	
Small Solaris App Server	Sun T2000 server with 4 core 1.2GHz UltraSparc T2 processor, 8GB Memory, 3x146GB disks	51,100	Est. 240
Solaris App Server	Sun T5220 server with 8 core 1.2GHz UltraSparc T2 processor, 32GB Memory, 3x146GB disks	250,500	449
Large Solaris App Server	Sun M4000 server with 4 quad core processors, 5MB on chip L2 cache, 32GB Memory, 2x73GB disks	255,000	Est 885
AIX Server	System p 550, 3x2-core 3.5 GHz POWER6 Processor, 6x146 GB 15K RPM SAS Disk Drive, 32 GB RAM	n/a	Est 900

STMS Hosting Services

SOW 5B

Shared File and Print Services

TABLE OF CONTENTS

1. SOW 5B, Scope and Summary

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in the Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them in this SOW.

1.2 Purpose of this Document

The purpose of this SOW is to generally describe the scope and functions of the Shared File and Print Services to be performed by Service Provider for the Province under the terms of the Master Services Agreement.

Section 1.5 (*Shared File and Print Services*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Shared File and Print Services, as indicated in the charts by an "R". The "Responsibility" charts are populated with "R" indicators that are to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.3 Onsite Support Services Overview

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating Manual*), 1.2.3 (*Server Locations, Transformation and Ownership*), and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference.

1.4 Shared File & Print Services Overview

This SOW describes the general scope and functions of the following components, which comprise the Shared File and Print Services (or "**SFP Services**") to be provided by Service Provider to the Province under the terms of the Agreement:

- Common Functions of Shared File and Print Services
- Shared File Services
- Shared Print Services

The services for each of the above-noted components are more particularly described in this SOW. The SFP Service is used by the Province and all Clients, as well as certain Broader Public Sector entities. New Clients and other Broader Public Sector entities may be added to the SFP Services through the Change Management Process or the Change Order Process, as applicable.

1.5 Shared File and Print Services

Service Provider will be responsible for delivery of the following Shared File and Print Services:

1.5.1 Common Functions of Shared File and Print Services

The Shared File and Print Services provide secure disk storage and file systems in which the Province and Clients store their data files, and a secure environment in which to print them. The SFP Services consist of a complex service that is critical to the daily operations of the Province, the Clients, and those Broader Public Sector entities who subscribe to this service. The SFP Service affects several stakeholders (such as the Service Provider Citrix server team for Citrix-provisioned LOB Applications, Province Citrix DTS team, Province Network infrastructure team, Province Active Directory team, Province Supported Workstation Services, Province supported Corporate Applications, Client Application support teams), and is subject to several dependencies, such as the following:

- the desktop re-direct to home drive;
- the home drive mapping in the "IDIR" ID profiles;
- the Active Directory (AD) objects for each SFP entity (such as servers, shares, print queues and DFS objects) in IDIR;
- hard-coded SFP server names in login scripts;
- the Province Network (SPAN/BC);
- the synchronization of print drivers with Citrix LOB, Citrix DTS; and
- 3PG and other external connections to SFP Servers.

The SFP Service includes the following (which is more fully described in Appendix I):

- file and print Server support;
- management of the file Server storage;
- file Server capacity and management of SFP supporting software;
- technical support for SFP access administration;
- data management operations (such as capacity trend reporting, group share splits, client share splits, Province and Client data migrations);
- SFP Client and Province incident and Change reports;
- Province and Client projects (such as physical office moves or reorganizations);
- daily backup of data files and folders and restores as needed;
- defined disaster recovery strategies for file and print failover in the event of a total Server failure or, in the case of file Servers, a partial but significant loss of data;

- File and Print Operations support during regular business hours (8:00am – 5:00pm) except where specifically described in the tables below;
- 24 x 7 Server support as described in the Server Management Services SOW;
- Incident and Problem Management and Change Management (with the exception of Level 1 Helpdesk functions which is provided by the Province);
- Service exclusions as listed in Appendix J.

As of the Hand-Over Date, the SFP Servers include both Tier 2 and Tier 3 Servers with performance and capacity management, all as described in the Server Management Services SOW. The SFP Services are not intended to include services for Application-related data (such as SQL or GIS files); in the event such Application data is found to exist on the file Servers, then the Service Provider will raise this matter with the Province (EHS) for resolution, failing which through the Governance Process for resolution. The Service Provider is not responsible for end-user support of Application Problems related to the files stored on the file Servers. The administration of the SFP Services among the Service Provider, the Province, Clients and applicable Broader Public Sector entities is described more fully in Appendix F – SFP Distributed Administration Model: Roles and Responsibilities.

Certain components of the SFP Services may be purchased through the Province Ordering System, and will either be provided by the Province's "Workstation Services Branch" (**WSS**) or the Service Provider. The Service Provider will receive requests to fulfill Province Ordering System orders for SFP Services either directly from Province Ordering System or from WSS through a generic mailbox (known, as of the Hand-Over Date, as the "**WTS Shared File Print**" mailbox). The Service Provider will monitor the WTS Shared File Print mailbox continuously each day for requests for SFP Services.

There are some Broader Public Sector entities and Clients who receive SFP Services from the Service Provider and whose desktop are not standard Province desktop, and whose desktop administration is not performed by the Province's "WTS Workstation Services" ID Administrators (although in some cases, WSS supports may support their workstations but not provide the ID Administrator function). SFP Service requests and SFP related Incidents for these Broader Public Sector entities and Clients may be handled using a different process, as more particularly described in the Midrange Operating Manual.

There are some Broader Public Sector entities and Clients who use the "SFPAPP" application and other SFP-provided tools and procedures, together with the appropriate privileged access to do their own SFP administration (such as create/modify/delete SFP Home Drives and group shares) (the "**Self-Managed Clients**"). Self-Managed clients do not order SFP Service through the Province Ordering System, and accordingly, the SFP Services provided to them by the Service Provider includes the creation of monthly reporting which is fed into the Province's Corporate Accounting System (CAS) for billing purposes by the Province.

The SFP Services under this SOW are intended to be Transformed, as more particularly described in the Transformation SOW. The required changes to the description of the SFP Services under this SOW as a result of such Transformation shall be documented as part of the transformation activities described in the Transformation SOW.

Common Functions of Shared File and Print Services	Province	Service Provider
Service Provider will provide the SFP Services in accordance with the performance standards outlined in Appendix I – SFP Performance Standards.		R
Service Provider will maintain, and redesign and update as required, a development and test environment to support the SFP Services.		R
Province (EHS) will provide Service Provider with advanced notice of the following regarding Province's and Client's business operational needs, to the extent the Province (EHS) is able to: <u>For Shared File Services</u> • circumstances, events or changes in business operations that could result in an increased demand for shared file storage capacity; • projected increases in personnel that could result in an increased demand for shared file storage capacity for the Province or any Client (or Broader Public Sector entity); • changes to the Remote Site locations; and • internal organizational changes <u>For Shared Print Services</u> • Material increase in the number of new print devices.	R	
Service Provider will procure, at its expense, share file Servers, print Servers, and share file print Servers, as and when necessary, to provide the SFP Services in accordance with this SOW.		R
Province will provide the Service Provider with the necessary access and authorization rights to the Province supporting SFP Applications (which are Province Proprietary Software, as defined in the Agreement) (the "**SFP Proprietary Software**") required for the Service Provider to access, use and modify the SFP Proprietary Software to deliver the SFP Services. For greater clarification, the Province will maintain the data administrator rights to the SFP Proprietary Software.	R	
Service Provider will update, maintain, patch and modify the SFP Proprietary Software as required to deliver the SFP Services, and will provide all such changes to the SFP Proprietary Software to the		R

Common Functions of Shared File and Print Services	Province	Service Provider
Province for purposes of maintaining the Province's data administrator rights up-to-date.		
Service Provider will provide the Province and Client personnel having elevated access and SFP administrative responsibilities (such as SFP Data Administrator or the Province Tier 1 Help Desk) with the following, during normal business hours: • bi-annual workshops/seminars with respect to SFP Applications, "SFPAPP" Application and other SFP-provided tools and procedures, and common issues/problems; and • assistance and training on an ad hoc basis and as required (which may be delivered on a one-on-one basis or as workshop/seminar), regarding SFP Applications and other SFP-provided tools and procedures, and the shared file directory structure used by the Service Provider to provide the SFP Services.		R
Service Provider will be responsible for selection of the facility and any travel and living costs for Service Provider personnel, and for the required facility, to host the SFP workshop/seminars or ad hoc sessions.		R
Develop and maintain SFP workshop/seminar training material as required for the use of ad hoc and bi-annual workshops/seminars		R
Province and Clients will be responsible for any related travel and living costs for their personnel and to attend the SFP workshop/seminars or ad hoc sessions.	R	
For purposes of facilitating efficient Incident and Problem escalation and resolution, Service Provider will use commercially reasonable efforts to develop, foster, and maintain cooperative working relationships with each of the Province Service Delivery Groups.		R
For purposes of facilitating efficient Incident and Problem escalation and resolution, Province will use commercially reasonable efforts to cause each of the Province Service Delivery Groups to develop, foster, and maintain cooperative working relationships with the Service Provider.	R	
To the extent that Service Provider requires access to the Province's systems and directories (such as IDIR) to perform its obligations and provide the SFP Services under this SOW, the Province will provide the Service Provider with that access, or will cause the applicable	R	

Common Functions of Shared File and Print Services	Province	Service Provider
Province Service Delivery Group to perform the required function (in lieu of giving Service Provider the access), as determined by the Province. Any disagreement between the Parties regarding the access to the Province's systems and directories that are required by the Service Provider to perform the SFP Services, then the Parties will resolve the matter through the Governance Process.		
Service Provider will maintain SFP shared directories and printers and all related and required information, in the Province's directory systems (such as IDIR, TIDIR), as more particularly described in the Midrange Operating Manual.		R
Province will maintain responsibility for the Distributed File Services (DFS) domain in Active Directory.	R	
Service Provider will manage the DFS objects contained in the DFS structure using methods more fully described in the Midrange Operating Manual.		R
Province will notify the Service Provider in advance of any major projects that are planned for the Province that will require integration with the SFP Services (such as the refresh of the Province's desktops) (each, a "**Major Project**").	R	
Service Provider will work with the Province and the Province Service Delivery Groups as may be required in the development of all applicable project management, communications, testing, problem escalation, problem resolution and implementation plans for the Major Projects ("**Project Plans**"), to the extent that such Project Plans require integration with the SFP Services.		R
Service Provider will perform such integration testing and problem resolution activities relating to the SFP Services as may be necessary, and working cooperatively with the applicable Province Service Delivery Groups and in accordance with the Project Plans, so that upon the completion of the Major Project, the SFP Services will be fully available and operational for the Province and the Clients affected by the Major Project.		R
The Province will provide the Service Provider with the "SFP Authorization Matrix" as of the Hand-Over Date.	R	
The Province or any Client may request a change to the SFP Authorization Matrix from time to time (when the Province or such Client is indicated on the SFP Authorization Matrix as having the	R	

Common Functions of Shared File and Print Services	Province	Service Provider
authority to make such requested changes).		
The Service Provider will update the SFP Authorization Matrix as required from time to time and provide it to the Province (EHS) in accordance with the procedures described in the Midrange Operating Manual.		R
Service Provider will obtain the Province's or the Clients' approval, as applicable, from those individuals identified in the SFP Authorization Matrix as persons who can provide such approvals, before responding to Province or Client requests for specific SFP Services.		R
Service Provider will perform Performance Monitoring and Reporting as defined in the Server Management Services SOW for the SFP Servers.		R
Service Provider will perform Capacity Planning as defined in Server Management Services SOW for the SFP Servers.		R
Service Provider will provide the Province and the Clients with the technical capability to restore their recently saved or deleted files (which, as of the Hand-Over Date, means maintaining the functionality that allows the Province and the Clients to perform such restores with a "right click" of their mouse and to go back to approximately 2 weeks). This service is limited by the technology available in the local redundant storage of the Server.		R
After transformation of the SFP Services, the Service Provider will update the SFP recovery plan as required to maintain the transformed SFP Services. Service Provider will test the SFP recovery plan in accordance with the Project Plan for the Transformation of the SFP Services.		R
Service Provider will perform annual testing of the SFP recovery plan in Service Provider's test environment for SFP. Such testing will be based upon the recovery of each SFP Server role (such as a file server, print server or a file/print server).		R
Service Provider will provide the Province (EHS) with the results of all SFP recovery plan tests at the request of the Province.		R
Service Provider will support and respond to all Priority 1 Incidents and Priority 2 Incidents (as defined in the Services Management SOW) relating to the SFP Service on a 24 x 7 basis.		R

Common Functions of Shared File and Print Services	Province	Service Provider
Service Provider will provide the Province with SFP reports listed in Appendix B – SFP Reports by the frequency listed in that Appendix, and by way of a secured electronic delivery channel acceptable to the Province.		R
Service Provider will provide to SFP Data Owners with incident reports, all as described in, and in accordance with, Appendix F.		R

1.5.2 Shared File Services

Shared File Services provides file service administration and Incident and Problem Management for file Servers.

The Shared File Services includes creating and maintaining the file shares and space on file Servers, file moves, share moves, share deletion, share additions, and working with Province Service Delivery Groups.

Shared File Services	Province	Service Provider
The Province (EHS) will provide Service Provider with notice of any internal reorganization within the Province or a Client that requires the movement of files, and information regarding the particulars of the reorganization as may be required by the Service Provider in order to perform the data migration.	R	
The Clients and Province will, in their discretion and to the extent possible, forecast their respective capacity requirements for Shared File Services to the Service Provider.	R	
Service Provider will perform data migration as required in connection with an internal reorganization within the Province or moves within a physical location, as required by the Province or a Client in connection with the movement of files, or as a result of ongoing file storage capacity management that is required to be able to save files in the ordinary course of their business operations.		R
Service Provider will perform the data migration working with the Province Service Delivery Groups to develop and execute data migration plans, and will execute the data migration plans in accordance with the Change Management Process.		R
Service Provider will provide sufficient and additional shared file capacity to meet the Province's and Clients' business requirements and to support their operations so that the Province and Clients will be able to save and retrieve files in the ordinary course of their		R

Shared File Services	Province	Service Provider
business operations. Prior to any Transformation of the SFP Services, this will include a significant amount of disk space balancing by way of share file splits (being the division of a file share into 2 or more file shares), and share moves, to be managed in accordance with the Change Management Process and working with the Province, Clients and any applicable Province Service Delivery Groups.		
The Province, Clients and Province Service Delivery Groups will work cooperatively with Service Provider, as applicable, in accordance with the Change Management Process to plan, approve, communicate and coordinate share file splits and share moves.	R	
The Service Provider will require that all Service Provider Personnel who have Privileged Accounts that could allow them to access any data or information relating to a project, program or other matter to which the *Statistics Act* (British Columbia) applies, take the oath referred to in Section 4 of that Act (or any successor provisions) prior to being given such Privileged Account. The Service Provider will implement and document processes and procedures to manage and track the Service Provider Personnel who taken the *Statistics Act* (British Columbia) oath, and will provide the Province with a list of such Service Provider Personnel indicating the dates on which they took the oath, as requested from time to time by the Province.		R
Service Provider will provide optional logging of files on a shared file Server, on a fee quoted basis, through the Province Ordering System Process for matters not otherwise logged by Service Provider as part of the Shared File Service.		R
Service Provider will provide new share locations as required by the Province and Clients following the Request Management Process (but not through Province Ordering System).		R
Service Provider will perform file restores as required by the Province and Clients following the Request Management Process (but not through Province Ordering System).		R
Service Provider will setup and maintain file share security and file system security for the Shared File Services by defining the top three levels of the file system hierarchy security.		R
Self-Managed Clients will maintain the file server directory hierarchy and related security for their Shared File Services for all	R	

Shared File Services	Province	Service Provider
levels of file system including the top three levels.		
The Province and the Clients will maintain the file server directory hierarchy and related security for their respective Shared File Services for all levels of file system except for the top three levels which is maintained by the Service Provider.	R	

1.5.3 Shared Print Services

Shared Print Services provides Windows based print queue administration and Problem Management for printer Servers and Print Queues, and includes:

- creating and maintaining the Print Queues hosted on print Servers (generally, these Print Queues are used by desktop users);
- purging and resetting print jobs;
- working with other Province and Province Service Delivery Groups; and
- associating printer drivers with Print Queues.

There are some non-Windows Servers (such as the mainframe, OpenVMS, and Citrix Servers) using some Print Queues. Service Provider is not responsible for printer problems related to the printer device hardware and firmware, desktops and Province network (SPAN/BC); however, Service Provider will be involved as needed to assist the Province in resolving print issues as they occur in relation to printer device hardware and firmware, desktops and Province network (SPAN/BC).

Shared Print Services	Province	Service Provider
Service Provider will provide the required Lead Times to the Province or the Clients, as applicable and as set forth in the Services Management SOW, and obtain prior authorization pursuant to the SFP Authorization Matrix, before making any changes to the Print Queues. Any such changes will be made through the Change Management Process.		R
Service Provider will create, delete and change Print Queues as requested by the Province and Clients, as applicable. Print Queue creation, deletion and other changes will be managed through the Request Management Process described in the Services Management SOW.		R
Service Provider will provide Print Queue administration and Incident and Problem Management for printer Servers and Print Queues.		R

Shared Print Services	Province	Service Provider
Service Provider will test and certify up to a maximum of fifteen new print device drivers each Contract Year (or such greater number as may be agreed to by the Parties in the Change Order Process), during normal business hours, as requested by the Province (EHS) for the purpose of introducing new print devices, which testing will include: • compatibility of print device drivers with the Citrix Farm; • desktop testing for standard Province desktop printing (including MS Word, MS Excel, MS Exchange); • negative interaction with other approved print device drivers; • negative effect on the performance of the printer Servers; • provide logical access to Service Provider's test lab for the Province or Client to test their shared multi-function devices (MFD) and to testing for Province (WTS) initiated changes; and • network (SPAN/BC) bandwidth usage. Service Provider will communicate the results and recommendations of its print device driver testing to the Province (EHS) once available.		R
Province will consider the Service Provider print device driver test results and recommendations prior to new print devices being deployed for Province or Client use.	R	
Service Provider will maintain a list of certified printer devices that includes Printer device particulars (such as manufacturer, model number, and so on), as well as a list of print device drivers that are compatible with the Citrix Farm.		R
Service Provider will update the list of certified printer device drivers as new printer device drivers are certified and as existing printer device drivers become obsolete and are no longer used by the Province or the Clients. Service Provider will provide the Province (EHS) with a copy of the list of certified printer devices upon request from time to time.		R
Service Provider will install new print device drivers that have been certified by the Service Provider each year, as required, on the print Servers.		R

Shared Print Services	Province	Service Provider
Service Provider will work with the Province and the Clients, as applicable, to provide necessary Print Queue information for the Province or the Client to establish printing as needed for their respective Applications.		R
Service Provider will configure the local Server print function.		R
The Province and Clients will provide Service Provider with requests to configure a new Print Queue and will provide the Service Provider with the necessary information required by the Service Provider to do so.	R	
Service Provider will set and maintain Print Queue configurations as required by the Province and the Clients.		R
Province will notify the Service Provider in writing when Print Queues can be removed from the print Servers.	R	
Upon the receipt of a written notice from the Province or Clients to remove a Print Queue, the Service Provider will remove the Print Queue through the Change Management Process described in the Services Management SOW.		R
Service Provider will provide Level 2 support for print Server and Print Queue Problem Management when the Level 1 service desk is unable to resolve the issue. Service Provider will work cooperatively with Province Service Delivery Groups as required to resolve printing Incidents and Problems.		R
Service Provider will perform Print Queue migration as and when required to provide the print services contemplated under this SOW and in accordance with the Change Management Process.		R
Service Provider will provide the Province (EHS) with information from time to time that is known to Service Provider regarding printing leading practices and other similar tips that could be used by the Province or Clients to improve the overall quality and delivery of the print services, for consideration and use by the Province (EHS) as it may determine in its discretion.		R
Service Provider will monitor Print Queues and will provide the Province with the SFP Print Queue report on a daily basis (as described in Appendix B – SFP Reports), and store the SFP Print Queue report in a Province specified location.		R

Shared Print Services	Province	Service Provider
Province will install the printer devices and provide printer device hardware support.	R	
Province will retain responsibility for print Incidents and Problems related to the printer device hardware and firmware, Province desktops and Province network (SPAN/BC).	R	

APPENDIX A – DEFINED TERMS / DEFINITIONS

Definable Term	Definition
Applications	Has the meaning given to it in the Server Management Services SOW.
Change Management Process	Has the meaning given to it in the Services Management SOW.
DFS	The distributed file system that offers wide area network (WAN) replication and simplified, fault-tolerant access to geographically dispersed files and abstract file shares from Servers to the Active Directory.
DTS	The desktop hosting service based upon Citrix and managed by the Province.
File and Print Operations	Those functions/tasks that are performed by the Service Provider's SFP Core Administrators (defined in Appendix F below) for the purpose of maintaining and delivering the SFP Service (such as data moves, Print Queue creation, file share creation). These functions/tasks do not include those related to the management of Server hardware, Operating Systems or the Server Management Services.
Home Drive	A file share dedicated to a single user.
ID Administrator	The function which manages access administration using the Province's Active Directory accounts and groups. The access administration can be for any shared service (such as SFP, Exchange, Shared Web). The function includes the create/modify/delete of the Active Directory accounts and groups, and the access administration function includes the population and management of the group memberships.
Incident	Has the meaning given to it in the Services Management SOW.
Midrange Operating Manual	Has the meaning given to it in the Server Management Services SOW.
Multi-Function Device or MFD	An office machine that incorporates the functionality of multiple devices in one (such as print, fax, copy, scan).
Operating System	Has the meaning given to it in the Server Management Services SOW.
Print Queue	A reserved file location on a Server for the purpose of sending print output files to a printer and the print driver associated with the printer.
Privileged Account	Has the meaning given to it in the Server Management Services SOW.
Province (EHS)	Has the meaning given to it in the Server Management Services SOW.

Definable Term	Definition
Province Ordering System Process	Has the meaning given to it in the Server Management Services SOW.
Remote Site	Has the meaning given to it in the Server Management Services SOW.
Server	Has the meaning given to it in the Server Management Services SOW.
Server Management Services	Has the meaning given to it in the Server Management Services SOW.
SFP	Means shared file and print.
SFP Core Administrator	Has the meaning given to it in Appendix F below.
SFP Data Administrator	Has the meaning given to it in Appendix F below.
SFP Data Approver	Has the meaning given to it in Appendix F below.
SFP Data Manager	Has the meaning given to it in Appendix F below.
SFP Data Owner	Has the meaning given to it in Appendix F below.
SFP Services	Means the services described under this SOW.
STMS Data Centre	Means the STMS Calgary Data Centre and the STMS Interior Data Centre (each as defined in the Data Centre SOW).

APPENDIX B – SFP REPORTS

The reports in this Appendix are Province existing reports as of Hand-Over Date and will be made available to the Service Provider as of Hand-Over Date.

- **SFP Consumption by Organization (Used for billing)**
  - Frequency: Monthly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- SFP Internal: (Detailed consumption summary by month for all orgs over one year)
  - Frequency: Monthly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- **"big share" reporting**
  - Frequency: Monthly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- Disk space consumption provided to WTS (also feeds into billing)
  - Frequency: Monthly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- Access reports
  - Frequency: Ad hoc but not greater than twice weekly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- File type reports
  - Frequency: Ad hoc, as requested
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- Trending reports (per server, total)
  - Frequency: Monthly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- SFP Print Queue Analysis report
  - Frequency: Daily, as requested
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)
- Count of print queues by Client organization, by server, and by driver
  - Frequency: Monthly
  - Format: Electronic and determined by Service Provider
  - Recipient: Province (EHS)

- Approved Print Drivers
    - Frequency: Quarterly
    - Format: Electronic and determined by Service Provider
    - Recipient: Province (EHS)
- City-Town/Server Location matrix
    - Frequency: Quarterly
    - Format: Electronic
    - Recipient: Province (EHS)
- Client/Server matrix
    - Frequency: Quarterly
    - Format: Electronic
    - Recipient: Province (EHS)
- Group memberships report
    - Frequency: Ad hoc but not greater than twice weekly
    - Format: Electronic
    - Recipient: Province (EHS)
- Security Analyser
    - Frequency: Monthly
    - Format: Electronic
    - Recipient: Province (EHS)
- SFP System Access Reporting – Quarterly (see Appendix G)
    - Frequency: Monthly
    - Format: Electronic
    - Recipient: Province (EHS)
- SFP Billing Report
    - Frequency: Monthly
    - Format: Electronic
    - Recipient: Province (EHS)

Alerts

- Availability of Servers (Server service and spooler service)
- File space availability (by file share)

APPENDIX C - SYSTEMS

Intentionally Left Blank

APPENDIX D - SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E - SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

APPENDIX F – SFP DISTRIBUTED ADMINISTRATION MODEL: ROLES AND RESPONSIBILITIES

The following stakeholders have roles and responsibilities related to successful data management.

SFP Data Owners

The SFP Data Owner is the person in the Province, Client or Broader Public Sector organization who has responsibility for the data residing on the shared file Servers. The data can be a whole file share or part of a file share. The SFP Data Owner makes decisions regarding who should have access, and what kind of access, to the data. The SFP Data Owner does not need to know the technical details of how the access is granted, but does need to be able to describe the access required to the data.

The SFP Data Owner may request access changes to the data for which the SFP Data Owner has responsibility. The SFP Data Owners work with SFP Data Approvers for the technical details relating to the SFP Data Owners responsibilities. There may be multiple SFP Data Owners in any one in the Province, Client or Broader Public Sector organization.

The SFP Data Owner and the SFP Data Approver may be a combined role.

The data in each SFP home drive is owned by the "home drive owner".

SFP Data Approvers

The SFP Data Approver is the person in the Province, Client or Broader Public Sector organization who is familiar with the organizations overall data and security requirements. It is important that the SFP Data Approver understands the SFP security structure, principles and standards. The SFP Data Approver is responsible for ensuring that the shared file folder structure meets the business needs of the organization.

The SFP Data Approver reviews and approves any required or suggested changes to organization's data in consultation with the applicable SFP Data Owners. There should be more than one SFP Data Approver for any one organization to ensure coverage for SFP Data Approver responsibilities is available when needed.

The SFP Data Owner and SFP Data Approver may be a combined role.

SFP Data Managers

The SFP Data Manager is more of a function than a specific person. A SFP Data Manager can be either a SFP Data Owner or a SFP Data Approver.

Every "home drive owner" is responsible for managing the data in their home drive. SFP Data Owners and SFP Data Approvers are responsible for the management of the data in group shares.

SFP Data Administrators

On behalf of the Province, Client or Broader Public Sector organization, the SFP Data Administrators perform the tasks required to process an approved change request from a SFP Data Approver or SFP Data Owner. If the task is unclear, the request doesn't meet the SFP standards or the request is not-standard,

then the SFP Data Administrator works with the SFP Data Approver and/or SFP Data Owner to find an acceptable solution within the SFP standards, in consultation with SFP Core Administrators if required.

On behalf of the SFP Core Administrators, the SFP Data Administrators maintain the SFP security standards and follow SFP leading practices in handling SFP data.

In the case of organizations that provides its own administration services (e.g., they do not receive their administration services from WTS), the SFP Data Approver and the SFP Data Administrator can be a combined role.

SFP Core Administrators

The SFP Core Administrator is a Service Provider role that defines, creates and maintains the infrastructure layer of the SFP Service. The SFP Core Administrator provides training and consultation support to SFP Data Administrators regarding the SFP standards and assists in escalated issue resolution.

The SFP Core Administrator role is never combined with other roles. The SFP Core Administrator is not responsible for data on the SFP infrastructure beyond ensuring that the data loads are balanced to prevent disks filling-up.

APPENDIX G – SFP ELEVATED ACCESS ROLES

SFP System Access Reporting – Quarterly will set forth the numbers and names of Service Provider Personnel in each of the following elevated access roles:

- **SFP Server Administrator** - full administrative access to Server in order to manage hardware, operate system, support applications; personnel access all parts of the Server via console, terminal server, root shares; personnel are also members of each Server's" Local Administrator group", which provides full administrative access to server; used only in disaster recovery situations, or when the server is not accessible via the network;

- **SFP Core Administrator** - full administrative access to all SFP shares on SFP file and print servers in order to support SFP application; creates/modifies/deletes containers, shares, queues for each ministry, troubleshoots problems, moves data across administrative boundaries;

- **SFP Backup Operator** - access to all SFP file backups in order to perform file restores from SFP backup servers and tapes; and

- **SFP Service Accounts** - used primarily for non-interactive access, used by automated processes, such as for disk space reporting, billing processes, directory synchronization processes. Occasional interactive access required for troubleshooting automated processes.

APPENDIX H– SFP CHANGES REQUIRING PROVINCE OR CLIENT APPROVAL

All SFP changes require approval of the applicable Province, Client or Broader Public Sector organization (as per the SFP Authorization Matrix). For any change requiring notification only, the affected Province, Client or Broader Public Sector organization has the option of deferring the change to a different date upon request to the Service Provider.

The SFP changes that require approval from the Province, Client or Broader Public Sector organization are as follows:

- **Share Moves**

  Share moves from one Server to another, where the organization has not yet been migrated to the DFS service approval. Share moves between partitions on the same Server or shares in DFS do not require approval (but do require notification).

- **Dedicated Server Changes**

  Dedicated Server changes outside the standard change window require approval. Dedicated Server changes during the standard change window do not require approval (but do require notification).

- **DFS Implementations**

  The project to migrate to DFS for the SFP namespace will be implemented one organization at a time. The impact to the Province, Client or Broader Public Sector organizations will be the same as for a share move from one Server to another and therefore require approval.

- **Province/Client Migrations To/From SFP**

  When a Client or Broader Public Sector organization is set up in SFP and its data is moved onto SFP, approval is required for the data moves. When a Province entity, Client or Broader Public Sector organization leaves the SFP Service and its data is moved off SFP, this can be performed by the organization itself, or by the Service Provider if the organization approves it through Province Ordering System.

- **Province/Client Projects for Included Services**

  This category of SFP change includes Province, Client or Broader Public Sector organization requested, organization-specific projects for services which are included in the SFP Service, such as large share splits, changing Print Queue defaults, assisting with data or Print Queue cleanups. Internal client reorganizations are in this category, involving organization-specific renames of SFP entities and data moves between organizations. Planning for these changes is usually done in conjunction with the requesting Province entity, Client or Broader Public Sector organization; however, as each change is scheduled and the plan is finalized, the organization must approve any change to the schedule or the plan.

APPENDIX I – SFP PERFORMANCE STANDARDS

Set forth below are the minimum performance standards for the SFP Services prior to the relocation of any SFP Servers and related storage to the STMS Data Centres, measured from an end-user perspective (between the end-user's desktop and the nearest SFP Server through the network (SPAN BC)).

The Parties acknowledge that through the Transformation of the SFP Services, as defined in the Transformation SOW, the Server locations will change. The Service Provider will host the Home Drives and Print Queues on the nearest network located SFP Server to the end-user as appropriate.

The standards set forth below are the Province's posted standards for its SFP Services prior to the Hand-Over Date. The Parties acknowledge that the Province generally achieved better performance than the posted standards in the lower mainland (greater Vancouver area), Victoria and in other locations, with noted exceptions (such as, for example (i) some Remote Sites, (ii) circumstances where Clients elected for business reasons to use a group share in a central location that prevented the posted standards from being achieved, (iii) insufficient network (SPAN/BC) capacity, and (iv) other external reasons beyond the control of the Province). Service Provider's objective is to maintain the standards actually achieved by the Province for the SFP Services and to provide the SFP Services in a manner that does not result in a material loss of the standards actually achieved by the Province prior to the Hand-Over Date. The Parties further acknowledge that the Province has not produced a baseline of the standards actually achieved for the SFP Services where they are different than the posted standards, and as a result, a material degradation in performance may be indicated, in part, by a significant increase in applicable Client or Broader Public Sector complaints that do not result from extraneous factors outside of the control of Service Provider.

Posted Standards

- 1 Mb file open/save - less than 6 seconds;
- 10 Mb file open/save - less than 60 seconds;
- 1 Mb file - time to start printing - less than 30 seconds; and
- 10 Mb file - time to start printing - less than 5 minutes.

The standards set forth above may be changed by the Parties through the Joint Technology Architecture Working Group in connection with the relocation of any SFP Servers and related storage to the STMS Data Centres.

APPENDIX J – SERVICE EXCLUSIONS

Set forth below are standards that are intended to be excluded from the SFP Services. If the Service Provider becomes aware of the use of any of the following excluded standards by the Province, a Client or Broader Public Sector organization, then the Service Provider will raise the matter with the Province (EHS), and if necessary may raise the matter through the Governance Process if necessary, for resolution. The Service Provider acknowledges that although the following standards are intended to be excluded from the SFP Services, they are several occurrences of the excluded standards that exist as of the Hand-Over Date.

- Management of client data (such as permission changes, deletion, data moves within a client partition);
- SFP data storage is limited to storing a user's data files, and not Client Applications or its data, other than the following Client Applications (which, for greater clarification, may reside on SFP Servers):
    - TRIM application and the WTS WAS "corporate" Application), and
    - S15 dedicated SFP Server) related to the ' project. At issue for Inquiry
- Examples of excluded Client Applications and its data:
    - Website content
    - Oracle database/content
    - SQL database/content
    - Client/server Applications
    - GIS
    - Provincial government common or shared Applications (such as CHIPS, CRMS)

STMS Hosting Services

SOW 5C

Web Hosting Services

Table of Contents

1. SOW 5C, Scope and Summary

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in the Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them.

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating Manual*), 1.2.3 (*Server Locations, Transformation and Ownership)*, and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference.

1.2 Purpose of this Document

The purpose of this SOW is to generally describe the scope and functions of the Web Hosting Services to be performed by Service Provider for the Province under the terms of the Agreement.

Section 1.4 (*Web Hosting Services*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Web Hosting Services, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.3 Web Hosting Service Overview

This SOW describes the general scope and functions of the following components of the Web Hosting Services to be provided by Service Provider to the Province under the terms of the Agreement:

- Shared Web Hosting Service
- Dedicated Web Service - Optional
- Common Web Hosting Services

1.4 Web Hosting Services

1.4.1 Shared Web Hosting Service

The Shared Web Hosting Service provides the implementation and maintenance required for hosting the Province's web applications, and is designed for static and dynamic Web environments, and typically supports Internet, Intranet or Extranet, Web servers, and Web application Servers. The Shared Web Hosting Service include the following (as described in the Server Management Services SOW):

- Performance Management
- Capacity Planning
- Extended Support Hour Enhancement - 7 x 24

Service Provider will deliver Shared Web Hosting Services using Shared Web Hosting Servers provided by the Service Provider that run a Microsoft Operating System and web services software (such as IIS).

Shared Web Hosting Services	Province	Service Provider
Client initiates request, following the Province Ordering System Process as described in Server Management Services SOW, for Shared Web Hosting Services.	R	
For Dynamic Shared Websites, Clients will request at least two shared websites, one for test and development, one for production.	R	
Client to supply configuration elements to Service Provider as required for Service Provider to configure the "Shared Web Hosting" website, such as: • website name • DNS name • External, Internal or Extranet requirement (business requirements) • Web Master Security Access • Storage requirements • File system security settings • Initial application ID Requirements (such as who the lead administrator is, their network ID).	R	
Service Provider will setup the "Shared Web Hosting" website based on the requirements provided by the Client.		R
Client to provide storage requirements for any web-Application changes on the Client's website.	R	

Shared Web Hosting Services	Province	Service Provider
Service Provider will monitor the Clients' websites to determine if the websites are available.		R
Service Provider will resolve website availability Problems related to IIS.		R
Where the Service Provider is notified, through monitoring or by other means, that a Shared Web Site has an availability Problem and it is not related to the Shared Web Hosting Server or the Shared Web Hosting Service, then the Service Provider will open an Incident ticket with the Province "Service Desk".		R
For those Clients affected by Shared Web Incidents, the Service Provider will notify the Clients on the Client Contact List (as defined in the Shared Database Services SOW).		R
Register the Client's website name (URL) in Province's Server registration system (DNS) following Province procedures and using Province owned tools, and following the procedures in the Midrange Operating Manual.		R
To allow the Client to implement its website and/or Web Application on a "Shared Web Hosting" website, the Service Provider will configure the "Shared Web Hosting" website software, which will include: • Creating the IIS instance website • Establishing host header names • Configuring top level folder security • Establishing log file configuration		R
Service Provider will maintain the administrative access to the Shared Web Hosting Servers.		R
On the Hand-Over Date the Province will provide Service Provider with the administrative access to the Shared Web Hosting Servers.	R	

Shared Web Hosting Services	Province	Service Provider
Service Provider will notify the Province (EHS) of any websites on the Shared Web Hosting Servers which are not viable in the Shared Web Server Hosting environment as a result of changes made by the Client to its website and/or web-Application, and will provide the Province (EHS) with detailed reason and particulars therefor ("**Website Notice**").		R
If the Province (EHS) agrees with the Website Notice, then the Province (EHS) will advise the Client and will cause the Client to either change its website such that the website it is suitable for the Shared Web Hosting Server environment, or to move the website to a Dedicated Web Hosting Server environment. If the Client agrees to move the website to a Dedicated Web Hosting Server environment, then the change will be processed by a request in the Province Ordering System.	R	
If the Province (EHS) does not agree with the Website Notice, then the Province (EHS) and Service Provider will work cooperatively to come to an agreement as to whether or not the website is suitable for the Shared Web Hosting Server environment, and will escalate the matter through the Governance Process for resolution if necessary.	R	R
Service Provider will detect, escalate, resolve, and perform root cause analysis (as described in Service Management SOW) for all Web Hosting Server software Incidents and Problems.		R
Province will provide SiteMinder configuration information to the Service Provider for the installation and configuration of the SiteMinder software agent.	R	
Service Provider will install and configure SiteMinder agent on Web Hosting Servers as required at the request of the Province.		R
Province will be responsible for the SiteMinder Application.	R	

1.4.2 **Dedicated Web Service – Optional**

The Dedicated Web Service installs and supports Web Hosting Server software (such as IIS) on a Dedicated Application Server, as an Optional Service.

Dedicated Web Service – Optional	Province	Service Provider
Clients will request a new Dedicated Web Services through Province Ordering System.	R	
Client will supply configuration elements to Service Provider as required for the Service Provider to complete the Web Hosting Server software installation on the Dedicated Application Server software, such as: • website name • DNS name • External, Internal or Extranet requirement (business requirements) • Web Master Security Access • Storage requirements • File system security settings • Initial application ID Requirements (such as who the lead administrator is, their network ID)	R	
Service Provider will coordinate the implementation of the Web Hosting Server software with the Client on the Dedicated Application Server through the Change Management Process.		R
To allow the Client to implement its website and/or Web Application on a Dedicated Web Hosting Server, the Service Provider will install and configure the Dedicated Web Hosting Server software, which will include: • Creating the IIS instance website • Establishing host header names • Configuring top level folder security • Establishing log file configuration		R

1.4.3 Common Web Hosting Services

The Common Web Hosting Services are the services provided to both Shared Web Hosting Service and Dedicated Web Service.

Common Web Hosting Services	Province	Service Provider
Service Provider will provide, install, upgrade, patch, configure, make performance adjustments, backup and restore all software, security, associated network and hardware components used to provide the Web Hosting Services.		R
The Client will request that a particular website be secured, such as using an SSL certificate, and any necessary related information to secure the website.	R	
Province will procure and maintain a pool of SSL certificates, and provide the Service Provider with licenses for the SSL certificates.	R	
Service Provider will perform installation of the SSL certificates.		R
Service Provider will work with the Client to resolve access and security issues relating to the Web Hosting Servers of the Client's website.		R
The Service Provider will apply and plan IIS patches for the Web Hosting Servers in accordance with Change Management Process described in the Service Management SOW, and where applicable the Security SOW.		R
Clients, at their discretion will test the Client' web-Applications and website content following the application of any patches by the Service Provider on the Web Hosting Servers.	R	
The Service Provider will adjust the Operating System and IIS parameters of the Web Hosting Servers to the extent possible and feasible for improving the performance of the Client's web-Applications and website content (tuning).		R
The Service Provider will adjust the Operating System and IIS parameters of the Web Hosting Servers to improve performance of the Web Hosting Servers and IIS.		R

Common Web Hosting Services	Province	Service Provider
The Service Provider will review Web Hosting Server Operating System and IIS product status and maintenance information to identify trends and Problems.		R
The Service Provider will review web products status and maintenance information to identify current related trends and potential Problems with the website software in use under this SOW. Service Provider will perform preventive maintenance to the Web Hosting Server Operating System and IIS, in accordance with the Change Management Process, to prevent known Problems.		R
Service Provider will provide the Province's Online Channel Office (or its successor) with sufficient privileges to the Web Hosting Servers to permit the Online Channel Office to obtain website statistics.		R
Service Provider will provide file system access to the Client to allow for installation, maintenance of website content for the Client's website.		R
Client will develop, install, maintain and test the configuration of all its web-Applications and website content.	R	
Service Provider will work closely with Client to resolve Client web-Application or website content Problems that may be related to the Web Hosting Server.		R
Service Provider will contact third party vendors of the Web Hosting Server software for technical support of Web Hosting Servers Problems as required.		R

APPENDIX A - DEFINED TERMS / DEFINITIONS

Definable Term	Definition
Dedicated Application Server	A Server that is dictated to a Client and that Client's Applications.
Dedicated Web Hosting Server	A web-Server that is dedicated to hosting a Client's website.
Dynamic Shared Websites	A website that retrieves its content from a Database.
Online Channel Office	Branch of the British Columbia Government responsible for the Province's web presence, And being the entity that produces website statistics for all Province websites. or its successor entity.
Shared Web Hosting Servers	A web-Server that hosts more than one Client's website.
Web Hosting Servers	A Server that hosts a website.

APPENDIX B – REPORTS

Monthly reports setting forth, for each website:

- File space usage, by website for each Client, to be delivered to each respective Client
- Availability of web service per Server, to be delivered to the Province
- Availability by URL for each Client, to be delivered to each respective Client and to the Province (EHS)
- Billing report, to be delivered to the Province (EHS)

Alerts to be delivered as set forth below:

- Availability of website (URL ping)
- Availability of web Server (standard server alert)
- 90% file space threshold (notify the Client)

APPENDIX C – SYSTEMS

Intentionally Left Blank

APPENDIX D - SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E - SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

STMS Hosting Services

SOW 5D

Virtual Hosting Services

TABLE OF CONTENTS

1. SOW 5D, SCOPE AND SUMMARY

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them.

1.2 Purpose of this Document

The purpose of this SOW is to generally describe the scope and functions of the Virtual Hosting Services to be performed by Service Provider for the Province under the terms of the Agreement.

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating* Manual), 1.2.3 (*Server Locations, Transformation and Ownership)*, and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference.

Section 1.3 (*Virtual Hosting Services Overview*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Server Management Services, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

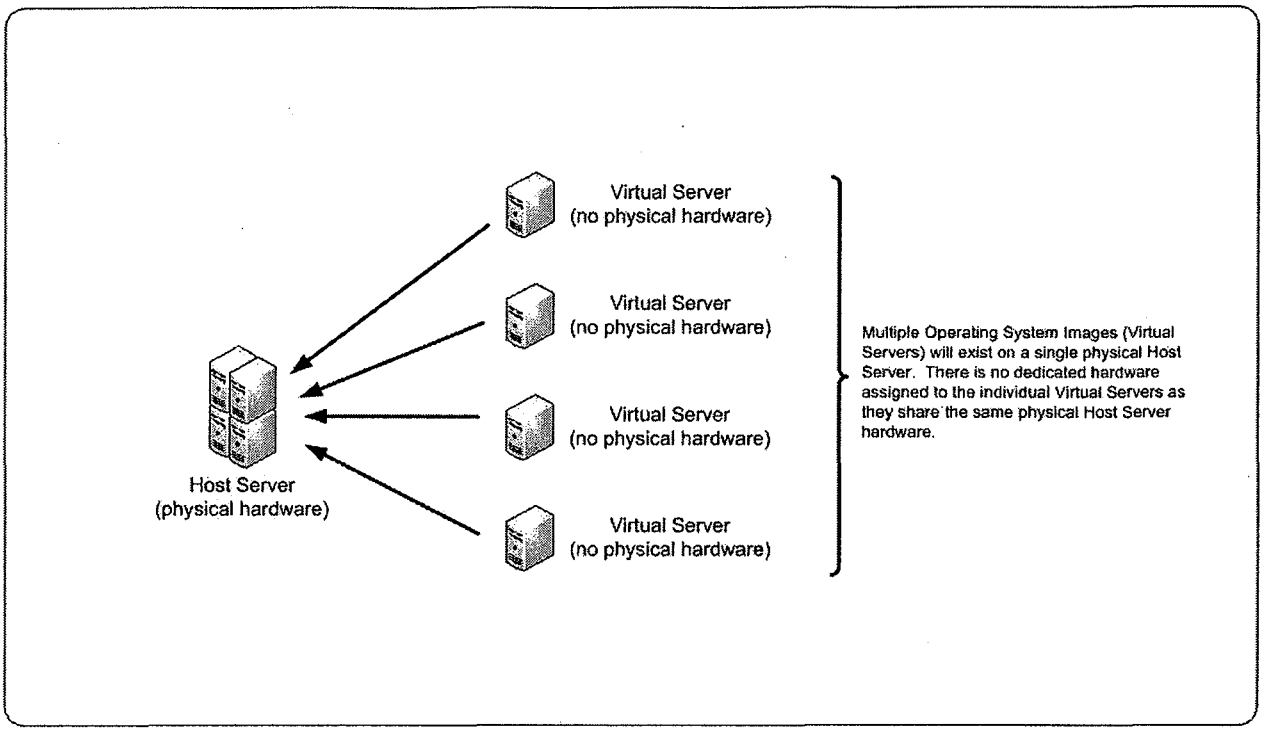
> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.3 Virtual Hosting Services Overview

1.3.1 General

Virtual Hosting Services provide the deployment and daily delivery of a Virtual Hosting environment, and include monitoring, maintaining, and managing hardware and system software configurations as defined in this SOW. The Virtual Hosting Services will only be provided from Province Data Centres and STMS Data Centres.

The Virtual Hosting Services environment is characterized by physical Host Servers and the Virtual Servers as illustrated in the diagram below.



Some of the key characteristics of the Virtual Server environment will be:

- rapid Virtual Server recoverability allowing the Virtual Server on a failed physical Host Server to be restarted rapidly on another physical Host Server;
- Virtual Servers will be distributed across the available physical Host Servers for the purpose of allowing improved utilization of the physical Host Servers;
- Virtual Server capacity load levelling will also result in Client Applications achieving improved performance; and
- Virtual Servers will allow Clients to request and receive Virtual Hosting Services on short notice and for short durations (such as months).

1.3.2 Virtual Transformation Plan

Service Provider will create a Transformation plan to migrate as many existing physical Servers as possible to Virtual Servers (the "**Virtual Transformation Plan**"). The Virtual Transformation Plan will be developed by Service Provider, in consultation with a Province and Client stakeholder group, working cooperatively and subject to the approval of the Province, all in accordance with the Transformation SOW. The Parties acknowledge that not all Servers are suitable for virtualization.

1.3.3 Excess Capacity Management for Physical Hosts

Service Provider will maintain Excess Capacity in the physical Host Servers for the purpose of achieving the Virtual Server Provisioning Service Levels, meeting short term use of Virtual Servers, and rapid recovery of Virtual Servers. The Excess Capacity will be based upon both the Server Farm Threshold and the Physical Host Threshold (both as defined below), such that when either the Server Farm Threshold or the Physical Host Threshold is achieved, the Service Provider will procure and use such number of additional physical Host Servers as are necessary to maintain the Excess Capacity in providing the Virtual Hosting Services.

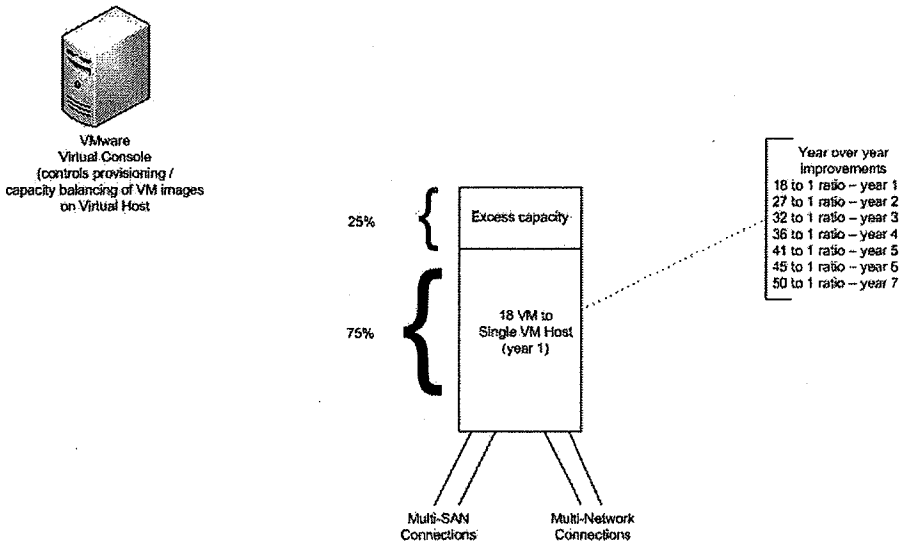
The Excess Capacity is intended to mitigate the occurrence of Unacceptable Utilization Trends. The Parties recognize that peak spikes in utilization rates of a physical Host Server for short durations of time (measured as seconds or less) will not alone result in the occurrence of Unacceptable Utilization Trends.

If as a result of the Physical Host Threshold and the Server Farm Threshold the Service Provider determines that it is accumulating unnecessary Excess Capacity as the number of physical Host Servers used in the Physical Host Farm increases, then the Service Provider may raise this matter with the Province, and the Parties will resolve it through Governance.

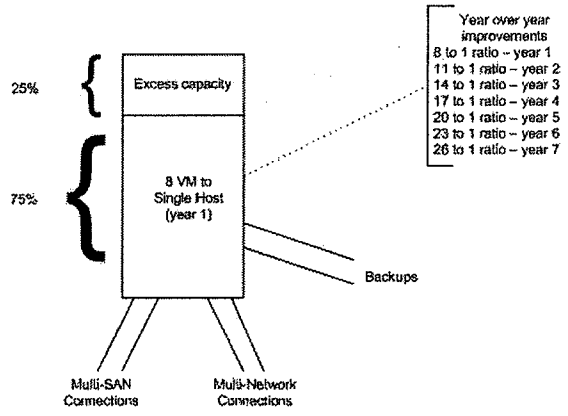
The Service Provider will monitor the physical Host Servers for Unsuitable Candidates based upon High Virtual Usage. The Parties recognize that peak spikes in a Virtual Server's use of a physical Host Server's capacity for short durations of time (measured as seconds or less) will not alone result in the occurrence of High Virtual Usage.

1.3.4 Number of Virtual Servers to a Host

The Service Provider acknowledges that it is assuming the risk of being able to host the number of Virtual Servers on a single physical Host Server illustrated in the Diagrams below. If the Service Provider is required to provisions additional physical Host Servers because it is not able to achieve the ratios set forth in the Diagrams below, then such additional physical Host Servers will be provisioned at the Service Provider expense, and will not be charged back to the Province.



Virtual Services (Windows and Linux)



Virtual Services (Solaris and AIX)

Upon the Hand-Over Date, Service Provider will support the Province's existing Virtual Servers and physical Host Servers (e.g. VMware, Solaris Containers, and AIX WPARs).

Service Provider will provide Virtual Hosting Services as described below.

Virtual Hosting Services	Province	Service Provider
The Province or a Client, as applicable, initiates a service request for a Virtual Server through to the Province Ordering System Process.	R	
Service Provider will assess the Province Owned Equipment under the Virtual Transformation Plan, and any service requests for a Virtual Server received pursuant to the Province Ordering System Process, to recommend Virtual Candidates to the Province.		R
The Province will approve the Service Provider's Virtual Candidate recommendations, and any disagreements on whether a Server is a Virtual Candidate will be resolved through Governance.	R	
Service Provider will procure physical Host Servers as required to maintain the Excess Capacity in providing the Virtual Hosting Services.		R
Service Provider will install, maintain and decommission physical Host Servers as required to provide the Virtual Hosting Services (subject to maintaining the Excess Capacity) following the process described in the Server Management Services SOW.		R
Service Provider will install, configure, maintain and retire Virtual Servers based on approved Province Ordering System requests following the processes described in the Server Management Services SOW.		R
Service Provider will establish and maintain the Privilege Accounts on the physical Host Servers in accordance with the privileged accounts management under the Server Management Services SOW. Privileged Accounts on the physical Host Servers are for the Service Provider to provide the Virtual Hosting Services, and as a result, these Privileged Accounts will not be given to, or created by, Clients.		R
Service Provider will implement processes and procedures to maintain Excess Capacity in the physical Host Servers used to provide the Virtual Hosting Services.		R
The Service Provider will implement processes and procedures, and will configure its monitoring agents on the physical Host Servers, to create a Problem Management Incident ticket upon the occurrence of an Unacceptable Utilization Trend.		R

Virtual Hosting Services	Province	Service Provider
Service Provider will provide the Province with web based access to the Server Farm Threshold and Physical Host Threshold reports described in Appendix B ("**Reports**"), at the times and frequency set forth in Appendix B.		R
If a single Virtual Server changes such that the Virtual Server achieves High Virtual Usage or operates an Unacceptable Application, then Service Provider will provide the Province (EHS) with information demonstrating that the Virtual Server has become an Unsuitable Candidate.		R
The Service Provider will work cooperatively with the Province (EHS) to determine an appropriate solution for either maintaining the Unsuitable Candidate as a Virtual Server or migrating it onto a physical Server, and if the Province (EHS) and the Service Provider are unable to agree upon an appropriate solution, then the matter will be referred to Governance.		R
The Province (EHS) will work cooperatively with the Service Provider to determine an appropriate solution for either maintaining an Unsuitable Candidate as a Virtual Server or migrating it onto a physical Server, and if the Province (EHS) and the Service Provider are unable to agree upon an appropriate solution, then the matter will be referred to Governance.	R	

APPENDIX A – DEFINED TERMS / DEFINITIONS

Definable Term	Definition
Excess Capacity	The unused capacity of a physical Host Server and the unused capacity of the Physical Host Farm.
High Virtual Usage	The point at which a single Virtual Server uses more than 75% of the memory (RAM), 75% of the CPU utilization, 50% of the network interface card, or 60% of the host bus adaptor (HBA) of its physical Host Server.
Host Bus Adapter (or HBA)	Device that connects a host system (the computer) to a storage network and storage devices.
Host Server	The physical Server on which Virtual Servers operate sharing the available resources of the physical Server.
Long Plateaus	The occurrence of plateaus in the physical Host Servers at or exceeding the Physical Host Threshold for periods measured in terms of hours.
Non-Peak Hours	Each calendar day between 17:00 and 08:00 hours.
Peak Hours	Each Business Day between 08:00 and 17:00 hours.
Physical Host Farm	The group of all of the physical Host Servers in a particular network at an STMS Data Centre that are used by the Service Provider at any particular time to provide the Virtual Hosting Services.
Physical Host Threshold	The achievement of any one of the following thresholds in each physical Host: (a) 90% utilization of the memory (RAM); (b) 90% utilization of the CPU utilization; (c) 60% utilization of the network interface card; or (d) 72% utilization of the host bus adaptor (HBA) utilization; and calculated in the manner described in Appendix XX for each physical Host Server used in the Physical Host Farm, and reported monthly showing the Peak Hour Daily Averages.
Random Access Memory (RAM)	Physical memory in a physical Server.
Server Farm Threshold	The achievement of any one of the following thresholds in the Physical Host Farm:

	(a) 75% utilization of the memory (RAM); (b) 75% utilization of the CPU utilization; (c) 50% utilization of the network interface card; or (d) 60% utilization of the host bus adaptor (HBA) utilization; and calculated in the manner described below for the Physical Host Farm (taken as the average of each physical Host Server used in the Physical Host Farm).
Short Plateaus	The occurrence of plateaus in the physical Host Servers at or exceeding the Physical Host Threshold for periods measured in terms of minutes.
Unacceptable Application	An Application that: (a) is not certified by the Application vendor for use on a Virtual Server; or (b) is included on a list of Applications agreed in writing by the Parties as being unacceptable for operation on a Virtual Server.
Unacceptable Utilization Trends	The consistent occurrence of either Short Plateaus or Long Plateaus or the occurrence of either Short Plateaus or Long Plateaus continually during any particular cycle (such as all day, all night, all weekend, the last couple of days of the month).
Unsuitable Candidate	A Virtual Server that is operating an Unacceptable Application or that achieves High Virtual Usage.
Virtual Candidate	(1) A Virtual Server request that will not operate any Unacceptable Applications; or (2) an existing Server that is not operating: (a) any Unacceptable Applications, and (b) at a utilization rate (having regard to the age of the Server and the Server's role in the Supported Infrastructure) that would likely result in the Server achieving a High Virtual Usage if it were migrated onto a physical Host Server, to the extent known.

APPENDIX B - REPORTS

Monthly report showing the following for the Physical Host Farm and for each physical Host Server:

- Peak Hour Daily Averages
  - Frequency: Weekly
  - Format: Electronic
  - Recipient: Province (EHS)
- Non-Peak Hour Daily Averages
  - Frequency: Weekly
  - Format: Electronic
  - Recipient: Province (EHS)
- Peak Hour Monthly Average
  - Frequency: Monthly
  - Format: Electronic
  - Recipient: Province (EHS)
- Non-Peak Hour Monthly Average
  - Frequency: Monthly
  - Format: Electronic
  - Recipient: Province (EHS)

APPENDIX C - SYSTEMS

Intentionally Left Blank

APPENDIX D - SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E - SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

APPENDIX F - HOST SERVER THRESHOLD CALCULATIONS

The Physical Host Threshold and the Physical Farm Threshold will be calculated as follows:

Peak Hours

(i) Each component threshold will be measured in 20 minute intervals during the Peak Hours (the "**Peak Hour Readings**");

(ii) the Peak Hour Readings will be used to calculate a daily average as follows (the "**Peak Hour Daily Average**"):

$$\text{Peak Hour Daily Average} = \frac{\text{Sum of the Peak Hour Readings in a Business Day}}{\text{Number of Peak Hour Readings in a Business Day}}$$

(iii) the Peak Hour Daily Averages will be used to calculate a monthly average as follows (the "**Peak Hour Monthly Average**"):

$$\text{Peak Hour Monthly Average} = \frac{\text{Sum of the Peak Hour Daily Readings}}{\text{Number of Business Day in the calendar month}}$$

Non-Peak Hours

(i) Each component threshold will be measured in 20 minute intervals during the Non- Peak Hours (the "**Peak Hour Readings**");

(ii) the Non-Peak Hour Readings will be used to calculate a daily average as follows (the "**Non-Peak Hour Daily Average**"):

$$\text{Non-Peak Hour Daily Average} = \frac{\text{Sum of the Non-Peak Hour Readings in a calendar day}}{\text{Number of Non-Peak Hour Readings in a calendar day}}$$

(iii) the Non-Peak Hour Daily Averages will be used to calculate a monthly average as follows (the "**Non-Peak Hour Monthly Average**"):

$$\text{Non-Peak Hour Monthly Average} = \frac{\text{Sum of the Non-Peak Hour Daily Readings}}{\text{Number of days in the calendar month}}$$

STMS Hosting Services

SOW 5E

Onsite Support Services

TABLE OF CONTENTS

Page

1. SOW 5E, SCOPE AND SUMMARY

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them.

1.2 Purpose of this Document

The purpose of this SOW is to generally describe the scope and functions of the Onsite Support Services to be performed by Service Provider for the Province under the terms of the Agreement.

Section 1.4 (*Onsite Support Services*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Server Management Services, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.3 Onsite Support Services Overview

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating Manual*), 1.2.3 (*Server Locations, Transformation and Ownership)*, and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference. Reference is also made to Part 3, WTS Remote Sites, of the Data Centre Services SOW.

1.4 Onsite Support Services

The Service Provider will perform the Services under the Services Management SOW, Server Management Services SOW and the Supporting SOWs remotely where appropriate and possible. Where the Service Provider is unable to do so remotely it will perform the Services Onsite in accordance with this SOW.

Where the Onsite Support Services is being provided through existing Province contracts (such as original equipment manufacturers' maintenance agreements for repair and maintenance of Province Owned Equipment) for Province Owned Equipment located at Province Midrange Facilities, the performance of the Onsite Support Services will be in accordance with the terms and conditions of the existing Province contracts.

"On-Site Support Services" consists of technical Onsite assistance and the performance of other Services at Province Midrange Facilities (such as and when required for installation, Service Requests in accordance with the Services Management SOW, Server repair, Problem and Incident resolution, removal and decommissioning of equipment and so on) and will be provided on an as needed basis.

Onsite Support Services	Province	Service Provider
Service Provider will dispatch a "Field Service Technician" to the Province Midrange Facilities as required to provide Services such as: • Server and related hardware installation • Service Requests • Server repair • Problem and Incident resolution • Removal and decommissioning of equipment		R
Service Provider will remove or decommission Province Owned Equipment and Service Provider Owned Equipment within a reasonable time, having regard to any known timing restrictions notified by the Province or a Client to Service Provider (such as the date on which the Province or Client must vacate leased premises).		R
The Province will maintain the Province Midrange Facilities as reasonably safe and clean facilities (with light and ventilation), to a standard that is no less than what the Province maintained prior to the Hand-Over Date.	R	
The Province will provide the Service Provider with access to the Province's "Regional Network Centre (RNC) Home Website" (the "**RNC Home Website**") containing certain information with respect to Province Data Centres, Regional Network Centres, and Remote Sites (such as security access information, floor plans, rack layout plans) (the "**Facility Information**"). The types of Facility Information provided in the RNC Home Website is not the same for each Province Midrange Facility location.	R	
The Province will maintain the Facility Information on the RNC Home Website and will update the Facility Information as required to maintain its currency.	R	
Service Provider will provide the Province with the particulars of any changes made by the Service Provider at a Province Midrange Facility that would result in the Facility Information being inaccurate, or any inaccuracies in the Facility		R

Onsite Support Services	Province	Service Provider
Information that otherwise become known to the Service Provider in performing the Onsite Support Services, so that the Province can update the Facility Information in the RNC Home Website.		
Service Provider will provide the Province with other relevant information regarding the Province Midrange Facilities that comes to the attention of Service Provider in performing the Onsite Support Services (such as safety issues, environmental issues, security issues, and so on).		R

APPENDIX A DEFINED TERMS / DEFINITIONS

Definable Term	Definition
Incident	Has the meaning given to it in the Services Management SOW.
Province Data Centres	Has the meaning given to it in the Server Management Services SOW.
Province Midrange Facilities	Has the meaning given to it in the Server Management Services SOW.
Province Owned Equipment	Has the meaning given to it in the Server Management Services SOW.
Regional Network Centres	Has the meaning given to it in the Server Management Services SOW.
Remote Sites	Has the meaning given to it in the Server Management Services SOW.
Server	Has the meaning given to it in the Server Management Services SOW.
Service Provider Owner Equipment	Has the meaning given to it in the Server Management Services SOW.

APPENDIX B REPORTS

Reports

Onsite usage:

- Frequency: Monthly
- Format: Electronic
- Recipient: Province (EHS)

APPENDIX C SYSTEMS

Intentionally Left Blank

APPENDIX D SUPPORTED CUSTOMER LOCATIONS

To establish a consistent Onsite Support Service for all Servers located at the Remote Sites the Onsite Support Service includes:

- a single Tier 3 - Remote Server Availability Service Level; and
- 7x24 Support.

The following table sets forth the cities where the Remote Sites are located, and where the Service Provider has Service Provider Personnel located, both as of the Hand-Over Date. The cities that are identified in the table as "Dispatch" are cities where the Service Provider does not have locally situated Service Provider Personnel (each a "**Dispatch Location**"), and accordingly, will require additional travel time by the Service Provider in performing the Onsite Support Services. The city from where Service Provider Personnel will be "Dispatched" is indicated in the table below where known.

The following conditions on dispatch and travel timing relate only to Server repair. Installation, upgrading and decommissioning of Servers will be performed following the Change Management Process as described in the Service Management SOW. Should a Remote Site be inaccessible due to the hours when the Location made be accessed by the Service Provider ("**Accessible Hours**"), or other conditions beyond the control of the Service Provider, the Service Level timing will commence once the "Field Service Technician" arrives at the location and is given access to the Province Midrange Facilities, provided that the Service Provider complies with the provisions in paragraphs (a) to (c) below.

For those Remote Locations have been identified as "Dispatch" in the table below:

(a) the Service Provider will notify the "Field Service Technician" to commence the "Dispatch" as soon as the determination for Onsite Services is made. The "Field Service Technician" will depart as soon as possible and no later than one day for those "Dispatch" Locations requiring extra time for travel plans, which may be made so that the timing of the departure and the travel time coincides with the Accessible Hours of the "Dispatch" Location. The travel plans of the "Field Service Technician" may consider the availability of flights or other commercial transportation necessary to travel to the "Dispatch" Location, will depart for the "Dispatch" Location within that time;

(b) when travelling to a Dispatch Location, the Service Provider will not detour to perform other unrelated services or tasks for itself, the Province or any other third party;

(c) the Service Provider will use all commercially reasonable efforts to complete the travel time to the Dispatch Location within the estimated dispatch travel times indicated in the table below; and

(d) subject to the Service Provider's compliance with the provisions of paragraphs (a) to (c) above, the Tier 3 – Remote Server Availability Service Level will be suspended until the Service Provider's "Field Service Technician" arrives at the Dispatch Location (and the calculation of the Service Provider's achievement of the Tier 3 – Remote Server Availability Service Level will be amended to account for such suspension).

The information set forth in the table below will be contained in the Midrange Operating Manual and will be updated as required from time to time. Any changes of a "Local" designation to a "Dispatch" designation will be subject to the approval of the Province.

City	Service	Estimated Dispatch Travel Time
Abbotsford	Local	
Alexis Creek	Dispatch - Williams Lake	4 hours
Atlin	Dispatch	
Bella Coola	Dispatch	
Burnaby	Local	
Burns Lake	Local	
Campbell River	Local	
Chilliwack	Local	
Clearwater	Dispatch - Kamloops	4 hours
Comox-Strathcona	Local	
Dease Lake	Dispatch	
Fort Nelson	Local	
Fort St. John	Dispatch – Dawson Creek	8 hours
Golden	Dispatch – Revelstoke	4 hours
Grand Forks	Dispatch – Castlegar	4 hours
Kamloops	Local	
Kelowna	Local	
Merritt	Dispatch – Kamloops	4 hours
Nanaimo	Local	
Nelson	Dispatch – Castlegar	4 hours
New Westminster	Local	

City	Service	Estimated Dispatch Travel Time
Port NcNeil	Dispatch - Campbell River	6 hours
Prince George	Local	
Prince Rupert	Local	
Queen Charlotte City	Local	
Saanich	Local	
Sechelt	Dispatch – Vancouver	24 hours
Stewart	Dispatch	
Surrey	Local	
Terrace	Local	
UBC	Local	
Vancouver	Local	
Victoria	Local	
Williams Lake	Local	

APPENDIX E SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

STMS Hosting Services

SOW 5F

Citrix Based Computing Services

TABLE OF CONTENTS

1. SOW 5F, Scope and Summary

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in the Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them.

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating Manual*), 1.2.3 (*Server Locations, Transformation and Ownership*), and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference.

1.2 Purpose of this Document

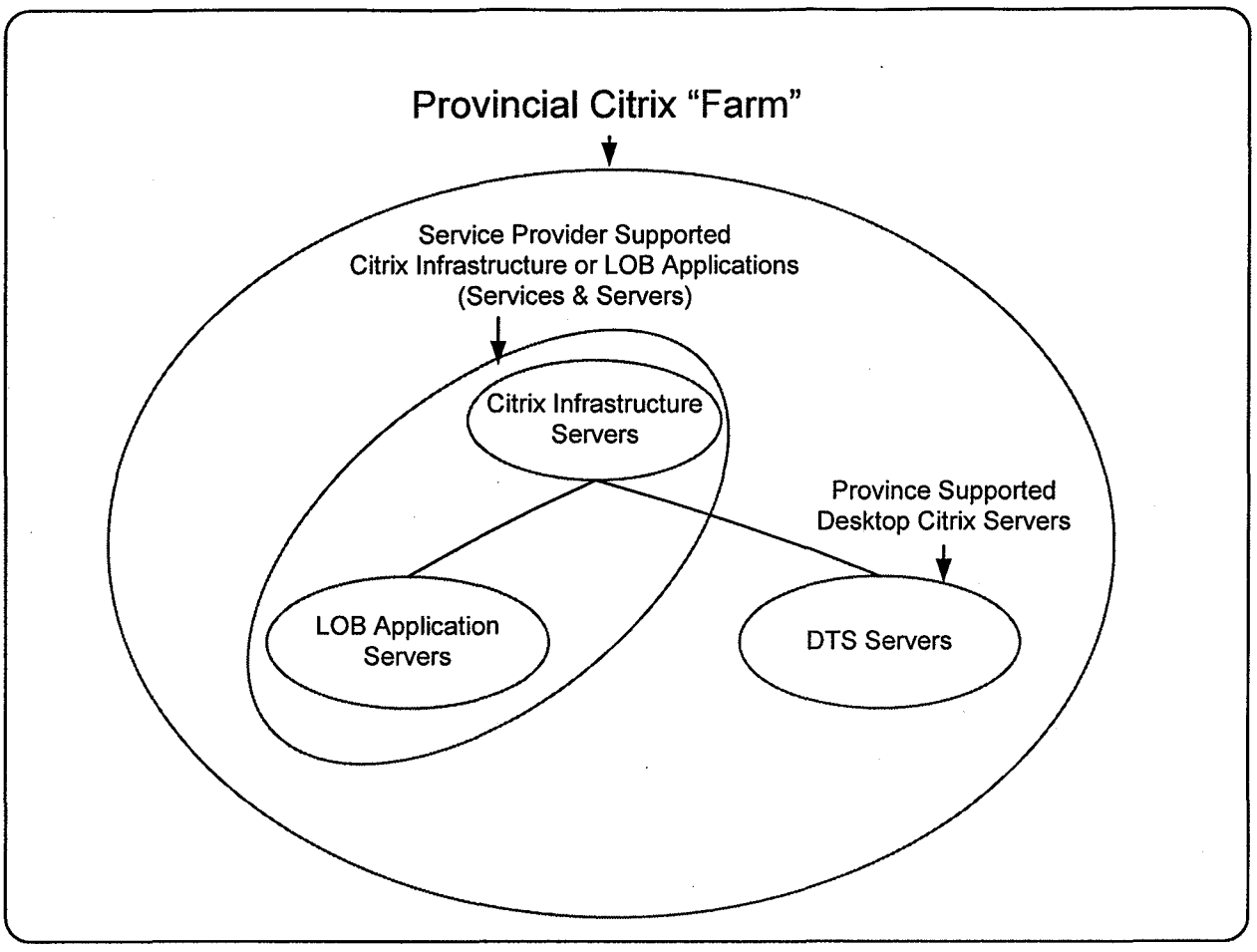
The purpose of this SOW is to generally describe the scope and functions of the Citrix Based Computing Services to be performed by Service Provider for the Province under the terms of the Agreement. Section 1.4 (*Citrix Based Computing Services*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Citrix Based Computing Services, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

> **R**esponsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

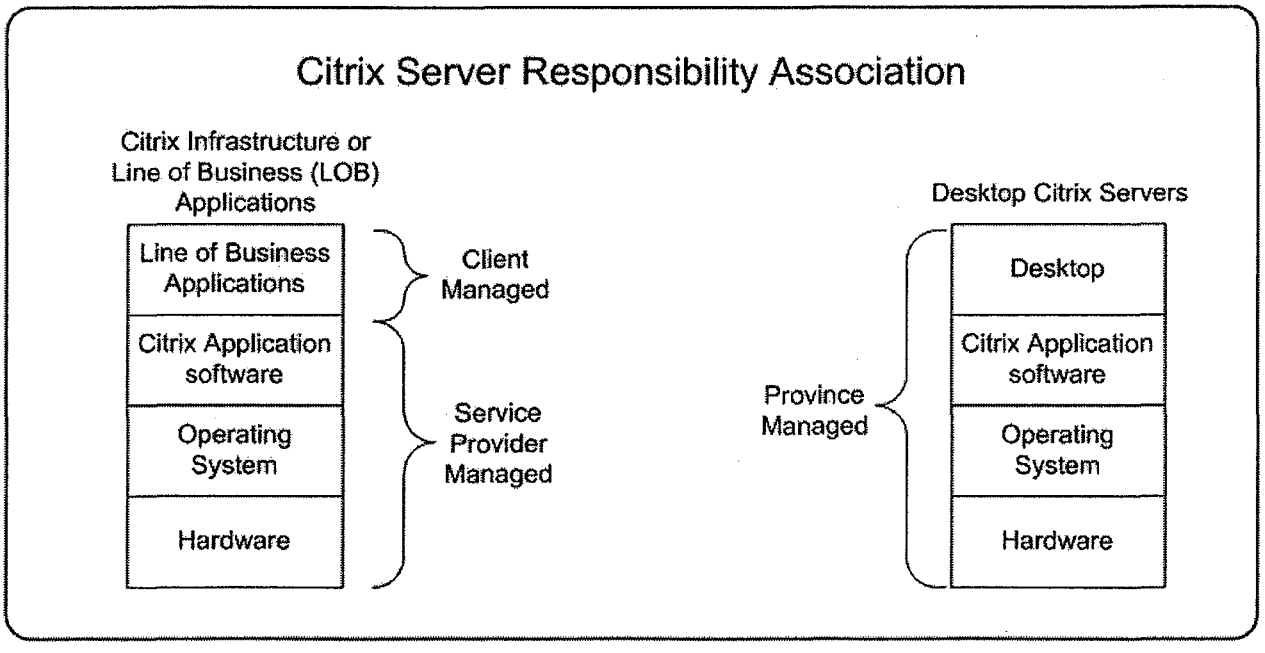
1.3 Citrix Based Computing Services Overview

This SOW describes the general scope and functions of Province's Citrix Farm administration, which comprises the Citrix Based Computing Services, to be provided by Service Provider.

"Citrix Based Computing" is a compute architecture that enables Application delivery to the Province's Clients. Citrix Servers in the Province's Citrix Farm have a standard configuration.



Province will install, configure and maintain Province Citrix Desktop Software



The Service Provider's Citrix Based Computing Services includes elements such as Presentation Server, License Servers, Web Interface Servers and capacity planning for the Citrix Infrastructure Servers. The Citrix Services in this SOW are for presenting Client Line of Business Application(s) and not the Desktop Citrix Servers.

1.4 Citrix Based Computing Services

The Citrix Based Computing Services are described more fully in the chart below.

Citrix Based Computing Services	Province	Service Provider
Client will provide a request for LOB Application hosting on a Citrix Server following the Province Ordering System Process, as described in the Service Management SOW and the Server Management Services SOW.	R	
Client will supply Service Provider with unique configuration elements, if any, as may be required for Service Provider to configure the Citrix Servers or Citrix Farm for the Clients LOB Application Hosting Services such as: • Security groups for the Client Application • Citrix Farm policies requirements • Citrix Server load balancing	R	
Service Provider will configure and install the Citrix Server based on the configuration elements provided by the Client, and as required to provide the LOB Application Hosting Services to the Client, in accordance with the Change Management Process and the Server Management Services SOW.		R
Client will install and maintain LOB Applications on the Citrix Server and notify the Service Provider when the LOB Applications are available for publishing.	R	
Service Provider will publish LOB Applications on the Citrix Server and will provide Client with notification of the publication.		R
Client will be responsible for third party licenses related to the LOB Applications.	R	
Service Provider will monitor the Citrix Servers to determine if they are available.		R

Citrix Based Computing Services	Province	Service Provider
Service Provider will resolve Citrix Server availability Problems related to the Citrix Service.		R
Where the Service Provider is notified, through monitoring or by other means that the Citrix Infrastructure Servers or LOB Application Servers have a performance or availability problem and it is not related to the Citrix Based Computing Services, then Service Provider will open an Incident ticket with the Province "Service Desk" and will notify the Client that an Incident ticket has been opened.		R
For purposes of facilitating efficient Incident and Problem escalation and resolution, Service Provider will use commercially reasonable efforts to develop, foster, and maintain cooperative working relationships with each of the Province Service Delivery Groups.		R
For purposes of facilitating efficient Incident and Problem escalation and resolution, Province will use commercially reasonable efforts to cause each of the Province Service Delivery Groups to develop, foster, and maintain cooperative working relationships with the Service Provider.	R	
Service Provider will work closely with Clients to resolve LOB Application issues that may be related to the Citrix software on the Citrix Servers.		R
The Service Provider will review Citrix product status and maintenance information to identify current related trends and potential Problems with the Citrix Services in use under this SOW.		R
The Service Provider will perform preventive maintenance to Citrix Servers to prevent known Problems in accordance with the Change Management Process.		R
Service Provider will debug, repair and resolve Citrix Server related Incidents and Problems following the Incident and Problem Management Process described in the Service Management SOW.		R
Service Provider will contact vendor for technical support on Citrix software Problems.		R
Service Provider will perform diagnostic activities to determine root cause of Citrix Server related Problems.		R

Citrix Based Computing Services	Province	Service Provider
Service Provider will monitor for and resolve Citrix Server alert conditions, using one or more of the following: • Microsoft Operations manager (MOM); • Citrix's monitoring capabilities; or • Service Provider's monitoring tools.		R
Service Provider will monitor Citrix and Microsoft Terminal Server licensing usage, and provide reports to the Province on a monthly basis.		R
Service Provider will establish a Citrix Infrastructure Server performance benchmark within 6 months of the Hand-Over Date.		R
Service Provider will recommend to the Province (EHS) when additional Citrix Infrastructure Servers are required to maintain Citrix Infrastructure Server capacity and performance.		R
Service Provider will provide support for the Citrix Infrastructure Server on a 7x24 basis.		R
Service Provider will install, manage configure, maintain, and decommission Citrix Infrastructure Servers and their related software (such as Operating System, Citrix Web Service, Citrix Licensing service, Database Servers as required).		R
Service Provider will remove the Citrix Server from the Citrix Farm, as requested by the Client, in accordance with Server Management Services SOW.		R
Service Provider will publish and and/or stop the publication of LOB Applications on the Citrix Server, as requested by Client.		R
Service Provider will monitor relevant Citrix bulletins for security-related patch alerts.		R
Service Provider will install and update Citrix software and Citrix patches, in accordance to the Change Management Process as described in the Service Management SOW and where applicable the Security SOW.		R

Citrix Based Computing Services	Province	Service Provider
Service Provider will test and report functionality of print drivers required for the Citrix Services (see the Shared File and Print Services SOW for the list of certified printers and print drivers for the Citrix Farm). Service Provider will attempt multiple print drivers that would work with the Client request printer to satisfy the Client's printer request.		R
Service Provider to inform the Client in instances where a suitable print driver cannot be found to satisfy the Client's printer request.		R
Service Provider will maintain the Citrix internet browser based software configuration settings on the Citrix Infrastructure Servers as requested by the Province.		R
Service Provider will participate in a "Citrix Working Group" established and chaired by the Province on a monthly basis. Service Provider participants will have a working knowledge and experience with the Citrix Services described in this SOW.		R
Province will coordinate, chair, and facilitate the Citrix Working Group with Service Provider and other applicable vendors.	R	

APPENDIX A - DEFINED TERMS / DEFINITIONS

Definable Term	Definition
Citrix Farm	The Citrix Servers that are logically associated to provide Citrix hosted Applications and desktop sessions. The Province's Citrix farm has three logical grouping of servers: the Citrix Infrastructure Servers, the LOB Application Servers and the DTS Servers.
Citrix Infrastructure Servers	The Citrix Infrastructure Servers consist of the Web Interface Servers, Zone Data Collector Servers, Citrix License Servers, Microsoft Terminal Server Licensing Servers.
Citrix Server	A Server running Citrix software and a member of the Citrix Farm.
Citrix Working Groups	A committee comprised of stakeholders involved in the managing of the shared Province Citrix Farm.
Desktop Terminal Service (DTS)	A desktop hosting service managed by the Province.
Line of Business (LOB) Application	A Client's business Application.

APPENDIX B – REPORTS

Reports

- Application usage reports (standard Citrix report), on a monthly basis to the Clients and the Province (EHS), and ad hoc as requested
- Availability of the Citrix Infrastructure servers, on a monthly basis to the Province (EHS)
- Citrix license usage, monthly to the Province (EHS)
- Terminal Server License usage, monthly to the Province (EHS)
- Billing Report

Alerts

- Availability of Citrix SQL server (standard DB alerting)
- Availability of the Citrix Infrastructure servers (standard Citrix alerting)
- Availability of web components (standard web alerting)
- Availability of Client LOB Applications Servers (standard Citrix alert)

APPENDIX C – SYSTEMS

Intentionally Left Blank

APPENDIX D - SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E - SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

STMS Hosting Services

SOW 5G

Shared Database Services

TABLE OF CONTENTS

1. STATEMENT OF CONFIDENTIALITY

1.1 Definitions and Interpretation

Capitalized terms used in this SOW will have the meanings given to them in the Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them.

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating Manual*), 1.2.3 (*Server Locations, Transformation and Ownership*), and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference.

1.2 Purpose of this Document

The purpose of this SOW is to generally describe the scope and functions of the Shared Database Service to be performed by Service Provider for the Province under the terms of the Agreement. Section 1.4 (*Shared Database Services*) of this SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Server Management Services, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.3 Shared Database Services Overview

This SOW describes the Shared Database Services to be provided by Service Provider to the Province and includes the following, which are more particularly described in this SOW and are available upon request through the Province Ordering System:

- Shared Database Services (Oracle, MS SQL)
- Shared Database Patch Management
- Shared Database Security Administration

1.4 Shared Database Services

Service Provider will be responsible for delivery of the following services:

1.4.1 Database Management Services

Database Management Services with respect to Shared Database environment includes the initial configuration and design of the Database structure, and management of the Database storage consumption and Shared Database availability.

For additional "Database Administration" services that are outside of the scope of this SOW, Clients may, at their discretion, obtain those services that are set out in the Application Enabling Services SOW.

For the Service Provider to provide the Database Management Services, the Province and Clients, as applicable, will be required to provide Service Provider with appropriate authorizations to interact with the Province's third party vendors (such as Oracle and IBM) under the Province's or Clients' vendor support agreements.

1.4.2 Database Management

Database Management provides the installation and support of the Relational Database Management System (RDBMS) on the Shared Database Servers. Database Management includes the following relational database products: Oracle and Microsoft SQL Server. Non-relational database technology is out of scope for the services provided under this SOW.

1.4.3 Shared Database Services (Oracle, MS SQL)

This Shared Database Service provides a secure, reliable environment for Databases on a Shared Database Server and includes Databases of multiple supported versions, backups, monitoring, licensing and a base allocation of managed storage for each Database Instance. Clients who choose to purchase this service must purchase a minimum of two Shared Databases (one Share Database for production and one Shared Database for test and development).

Shared Database Services provides support for Oracle and Microsoft SQL Server databases and includes 5GB of storage (additional GBs are provided at a per GB rate).

Service Provider will perform Database Administration tasks as detailed in the Midrange Operating Manual.

Shared Database Services (Oracle, MS SQL)	Province	Service Provider
Service Provider will develop and maintain the Shared Database Services design in accordance with the architecture provisions described in the Server Management Services SOW.		R
The Client will request new Shared Database Services through the Province Ordering System, as described in the Server Management Services SOW.	R	
Province (EHS) reviews and validates the order with in the Province Ordering Systems and will validate that: • The service request is within the scope of the Shared Database Services described in this SOW. • Clients request at least two Shared Databases, one for test and	R	

Shared Database Services (Oracle, MS SQL)	Province	Service Provider
development, one for production.		
Client to supply initial Database specifications to Service Provider to create the Share Database structure such as: • Database name; • Database version and patch set level; • Operating System requirement (if applicable); • Database storage (such as names of database tablespaces and size); and • Database backup requirements.	R	
Service Provider will create the Shared Database structure based on the specifications provided by the Client.		R
Service Provider will create one privilege administrative ID per Database to give the Client the ability to manage: • database objects • dataloads • userid access		R
Service Provider will monitor the Database for availability.		R
Service Provider will resolve Database availability problems related to the Shared Database Service.		R
Service Provider will maintain and update a list of contacts from client organization (the "**Client Contact List**") identifying the Province and Client organization staff for the Shared Database, and provide the Client Contact List to the Province (EHS) from time to time as requested.		R
Where the Service Provider is notified, through monitoring or by other means, that a Shared Database has availability problems and it is not related to the Shared Database Server or the Shared Database Service, then the Service Provider will open an Incident ticket with the Province "Service Desk".		R

Shared Database Services (Oracle, MS SQL)	Province	Service Provider
For those Shared Database Clients affected by Shared Database Incidents, the Service Provider will notify the Clients on the Client Contact List of the Incident.		R
Client will provide data management (such as logical data administration, data cleansing/scrubbing, data manipulation, and so on) with respect to the Client's data residing in its Shared Database.	R	
Service Provider to provide alerts to Client before the Client's Shared Database reaches its storage threshold.		R
Client will request additional storage through the Province Ordering System. If Shared Database Service interruptions are due to Clients not ordering sufficient storage, despite Service Provider storage threshold notifications, then Service Provider will not be held accountable for those Shared Database Service interruptions.	R	
Service Provider will notify the Province (EHS) of any Databases on the Shared Database Servers which are not viable in the Shared Database Server environment as a result of changes made by the Client to its Database, and will provide the Province (EHS) with detailed reasons and particulars for why such Databases are not viable for the Shared Database Server Environment ("**Database Notice**").		R
If the Province (EHS) agrees with the Database Notice, then the Province (EHS) will advise the Client and will cause the Client to either change its Database such that the Database it is suitable for the Shared Database Server environment, or to move the Database to a dedicated Server. If the Client agrees to move the Database to a dedicated Server, then the change will be made through Province Ordering System.	R	
If the Province (EHS) does not agree with the Database Notice, then the Province (EHS) and Service Provider will work cooperatively to come to an agreement as to whether or not the Database is suitable for the Shared Database Server environment, and will escalate the matter through the Governance Process for resolution if necessary.	R	R
Clients will approve all changes to their Databases related to Database upgrades and patching following the Change Management Process.	R	

Shared Database Services (Oracle, MS SQL)	Province	Service Provider
Service Provider to install, upgrade, patch, remove and configure Database on the Shared Database in accordance to the Change Management Process.		R
Service Provider to install, upgrade, patch, remove and configure Database related backup and restore tools on the Shared Database in accordance with the Change Management Process.		R
Service Provider will install, upgrade, patch, remove and configure Service Provider management and monitoring tools in accordance with the Change Management Process.		R
Migrate/upgrade Database to the current version after Database upgrades in accordance to the Change Management Process.		R
Service Provider will perform scheduled backup services with respect to the Databases on the Shared Database Servers to meet the "Recovery Point Objective" of the previous business day, to the extent possible.		R
Service Provider will perform restore services as required and when requested by Clients with respect to the Databases on the Shared Database Servers, to meet the "Recovery Point Objective" of the previous business day, to the extent possible, in accordance with the Change Management Process.		R
Clients, at their discretion, will test their Databases in conjunction with their Application following any Service Provider Database upgrades or after the application of any Database patches.	R	
Service Provider will add and remove Database storage on the Shared Database Server through the Change Management Process.		R
Service Provider will provide monthly reports described in Appendix B through a reporting website as described in the Server Management Services SOW, or such other means as agreed to by the Parties.		R
Client to manage Database objects and Application user access in relation to their Databases.	R	
Service Provider will perform Database Administration tasks as detailed in the Midrange Operating Manual.		R

Shared Database Services (Oracle, MS SQL)	Province	Service Provider
Service Provide will perform such tasks and functions as are reasonably necessary and that are generally followed within the industry in respect of Database management to maintain Database performance (such as running an Oracle Database statistical package on the Oracle Shared Databases).		R
The Service Provider will review Database product status and maintenance information to identify current related trends and potential problems with Database. Service Provider will perform preventive maintenance on the Database to prevent known problems in accordance with the Change Management process.		R
Service Provider will resolve Database related Incidents and Problems following the Problem Resolution Process, and will perform root cause analysis as necessary.		R
Service Provider will contact the vendors for technical support on Database software issues.		R
Service Provider will for monitor and resolve Database alert conditions.		R
Service Provider will perform Database capacity planning for the Shared Databases to ensure, to the extent that the Service Provider is able, that there is sufficient physical memory (RAM) and processor capacity on the Shared Database Servers to perform the Shared Database Services. The Service Provider capacity planning will not be able to predict increases due to material changes in the Database use.		R
Service Provider will remove Database Instances as requested by the Client through the Province Ordering System.		R

1.4.4 Shared Database Patch Management

The Shared Database Patch Management services describes Service Provider's responsibility for monitoring and planning for security and functional database patches as required to provide the Shared Database Services and as required under the Security SOW. The Shared Database patches will be in accordance with the Change Management Process.

The Shared Database Patch Management services are described more fully in the chart below.

Shared Database Patch Management	Province	Service Provider
Service Provider will monitor for relevant Database patches and industry bulletins for related patch alerts.		R
The Service Provider will plan and apply patches for Shared Databases in accordance with Change Management Process, and where applicable the Security SOW.		R
Service Provider will apply patches to Shared Database as required to maintain vendor support and to comply with the Security SOW.		R
Clients, at their discretion, to provide necessary testing of Clients' business Applications following any Service Provider Shared Database patch installation.	R	

1.4.5 Shared Database Security Administration

Database Security Administration provides support for the installation and maintenance of the Database on Shared Database Servers.

Database Security Administration	Province	Service Provider
Service Provider will implement and maintain Database security as required under the Security SOW and the Province Security Policies & Standards.		R
Service Provider will notify the Province (EHS) of any Security Events or Security Incidents relating to the Databases, as described more fully in the Security SOW.		R

APPENDIX A – DEFINED TERMS / DEFINITIONS

Definable Term	Definition
Database (DB)	A set of files where application data (the reason for the database), meta-data is stored in a computer system.
Database Administration	The administration of a Database that deals with the Database as a whole up to and including the tablespaces.
Database Instance	Software (and memory) used to manipulate the data in a Database.
Shared Database	A Database that resides on a shared Server.
Shared Database Servers	A Server that hosts a Shared Database.

APPENDIX B – REPORTS

Monthly reports on the following, by Database and by Shared Database Server:

- Availability of Database (to both the Province (EHS) and the Client)
- File space usage by Database (to the Client)
- Database license usage – to the Province (EHS)
- Billing report

Service Provider will deliver alerts as follows:

- Availability of Databases
- 90% file space threshold (notify the Client)

APPENDIX C – SYSTEMS

Intentionally Left Blank

APPENDIX D - SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E - SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

STMS Hosting Services

SOW 5H

Application Enabling Services

TABLE OF CONTENTS

1. SOW 5H, Scope and Summary

1.1 Definitions

Capitalized terms used in this SOW will have the meanings given to them in the Appendix A of this SOW, and as defined in the other SOWs, the Agreement and the Master Transfer Agreement, as applicable. Any terms defined elsewhere in this SOW will have the meanings given to them.

The provisions of the Sections of 1.2.1 (*General*), 1.2.2 (*Midrange Operating Manual*), 1.2.3 (*Server Locations, Transformation and Ownership*), and 1.2.4 (*Use of Province Ordering System, ITIMS and Request Management*), of the Server Management Services SOW are incorporated into this SOW by reference.

1.2 Purpose of this Document

The purpose of this SOW is to generally describe the scope and functions of the Application Enabling Services to be performed by Service Provider for the Province under the terms of the Agreement. Some sections in this SOW include "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Application Enabling Services, as indicated in the charts by an "R", to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified, but only to the extent requested by the Client, acknowledging that the level of involvement of the Service Provider will vary from Client to Client for similar tasks, as determined by each particular Client through the Province Ordering System Process.

1.3 Application Enabling Services Overview

The Application Enabling Services under this SOW are available upon request through Province Ordering System at the discretion of the Clients, and will be documented in writing (as a statement of work) between the Service Provider and the Clients at the time of purchase. For greater clarification Clients may, at their discretion, purchase similar services to some or all of the Application Enabling Services from any other party instead of ordering them from the Service Provider under the Province Ordering System.

This SOW describes the Application Enabling Services that will be provided by Service Provider when requested through the Province Ordering System, and includes the following:

- Database Management Services – Optional
- Middleware Support - Optional
- Application Release Management Services – Optional

1.3.1 Database Management Services – Optional

Service Provider will perform the following relational Database Management Services for the Province which includes Database Services for only Oracle, DB2, MS SQL (or their successor products). Non-relational database technology, and Logical Database Administration, are out of scope for the Database Management Services provided under this SOW.

The Database Management Services requested by Clients under this SOW may consist of any or all of the components of the Application DBA Roles and the Physical DBA Roles (as defined below).

1.3.2 Middleware Support – Optional

Service Provider will perform the following Middleware Support Services for the Province for the products listed in Appendix F. Any addition of new products or changes to the existing products in Appendix F (including recognition of successor products) will be made with the consent of the Province through the Change Order Process.

Middleware Support does not include Application development services using the Middleware software.

1.3.3 Application Release Management Services – Optional

Service Provider will perform the following Application Release Management Support Services as requested by Clients. This includes:

- setting Application environment configuration
- Release Management
- starting and stopping Application
- monitoring the execution of applications
- application backups and restores

Application Release Management Support does not include Application development services.

1.4 Database Management Services – Optional

Service Provider will deliver the following Database Management Services, as and to the extent requested by Clients through the Province Ordering System:

Database Management Services	Province	Service Provider
Client initiates request for Database Management Services through the Province Ordering System Process. Clients may, at their discretion, arrange for a draw-down account to be used by the Service Provider where the amount of work required by the Client cannot be ascertained.	R	
Service Provider will provide the Database Management Services purchased by Client through the Province Ordering System.		R
Service Provider will provide the Province (EHS) and the Client with a monthly report describing the general Database Management Services performed in the prior month and the associated costs to the Client, together with a description of any variances from the original estimate of effort and cost and the reasons for the variances.		R
Service Provider will manage any Database Management Services that could affect the availability of any Applications through Change Management Process.		R
To the extent possible, and without recourse for failure to do so, Client will notify the Service Provider of any business requirements that could affect future Database growth.	R	
Client will report and provide information to the Service Provider regarding Database Problems.	R	
The Service Provider will monitor Relational Database Management System (**RDBMS**) product status and maintenance information to identify current related trends and potential issues with the RDBMS in use under this SOW.		R
Client will provide the Service Provider with the Client's production Database change window requirements specific to the Client's business requirements.	R	
Service Provider will evaluate the need for patches deemed critical by the software vendor to support RDBMS products to mitigate known Problems.		R

Database Management Services	Province	Service Provider
Service Provider will install all RDBMS patches through the Change Management Process.		R
Service Provider will implement and maintain Database security as required pursuant to the Security SOW and the Province Security Policies & Standards.		R
Service Provider will the Province (EHS) of any Security Events or Security Incidents relating to the Databases, as described more fully in the Security SOW.		R

1.5 Middleware Support - Optional

Middleware Support is the operational and management processes and support of Middleware managed by AES (see Appendix G). Service Provider will deliver the following Middleware Support Services as to the extent requested by Clients through the Province Ordering System.

Middleware Support	Province	Service Provider
Client will initiate a request for Middleware Support Services through the Province Ordering System Process.	R	
Service Provider will provide the Middleware Support Services purchased by Client through the Province Ordering System.		R
Service Provider will provide the Province (EHS) and the Client with a monthly report describing the general Middleware Support Services performed in the prior month and the associated costs to the Client, together with a description of any variances from the original estimate of effort and cost and the reasons for the variances.		R
Service Provider will manage any Middleware Support Services that could affect the availability of any Applications through Change Management Process.		R
To the extent possible, and without recourse for failure to do so, Client will notify Service Provider of changes in business requirements that could affect future use of Middleware software.	R	
To the extent possible, Client will report and provide information regarding Middleware software Problems.	R	

Middleware Support	Province	Service Provider
The Service Provider will monitor Middleware software status and maintenance information to identify current related trends and potential issues with the Middleware software in use under this SOW.		R
Client will provide the Service Provider with the Client's production Middleware change window requirements specific to the Client's business requirements.	R	
Service Provider will evaluate the need for patches deemed critical by the software vendor to support Middleware software to mitigate known Problems.		R
Service Provider will install all Middleware patches through the Change Management Process.		R
Service Provider will implement and maintain Middleware security as required pursuant to the Security SOW and the Province Security Policies & Standards.		R
Service Provider will notify the Province (EHS) of any Security Events or Security Incidents relating to the Middleware, as described more fully in the Security SOW.		R

1.6 Application Release Management and Support Services – Optional

Application Release Management Support Services covers the following services:

- Provide a holding or staging area for the Application releases to be promoted; and
- Move the Application releases from the holding or staging area to the target environment (such as from a Development environment to a Test environment, a Test environment to a Production environment, Test environment to Training environment, Test environment to Education environment).

These services are performed under Change Management Process. This service does not include quality assurance testing (such as the inspection, testing, or checking of the Application release), other than to ensure that the Application release is as specified in the Change Request.

Service Provider will deliver the following Application Release Management and Support Services as and to the extent requested by Clients through the Province Ordering System.

Application Release Management Support Services	Province	Service Provider
Client will maintain and provide to the Service Provider the Client Contact List (as defined in the Shared Database SOW).	R	
Client will provide the Service Provider with the Client's Application environment requirements such as file system allocation, size and directory structures (including development, test, education/training and production).	R	
Service Provider will create, configure and manage the Client's Application environment according to client specification.		R
Client will: • define, develop, provide and schedule Application enhancement and releases; • perform Application release coding, enhancement and unit testing, integration testing; • perform Application release quality assurance testing; • provide application release bundle, migration instructions and install scripts for Application release migration; • perform Application problem determination (process, bugs and data) and resolution; • perform Application performance tuning; • provide Application security requirements such as groups and ownership IDs.	R	
Service Provider will perform Application release migrations to test, education, training and production environments according to Client instructions.		R
Service Provider to stop and start Application(s) in development, test, education, training, production or other environments, as requested by the Client.		R
Service Provider will create and manage Middleware Application security according to the Client's specification.		R

Application Release Management Support Services	Province	Service Provider
Service Provider will perform security and administrative tasks to support Client's Application development and testing teams (such as manage developer and tester IDs and group access).		R
Service Provider will work with the Client to maintain Application production change windows that meets the Client's business requirements.		R
Service Provider will perform backup and recovery for the Application environment as requested by Client.		R
To the extent possible, Service Provider will provide input on hardware and software changes that might affect the Client's Application environment.		R
Service Provider will monitor and report to the Client on Application storage, CPU and memory capacity based on thresholds set by Service Provider as requested by Client.		R
Service Provider will allocate storage and plan future growth based on requirements provided by the Client.		R

APPENDIX A – DEFINED TERMS / DEFINITIONS

Term	Definition
Middleware	Middleware is computer software that connects software components or Applications, for the purposes of this SOW Middleware software consists of the software listed in Appendix F (and their successors).
Logical DBA (Data Base Administrator)	The Logical role of a DBA involves defining the logical data model for the Database. Defining the Database layout including table and column definitions, table relationships, size, and such would be all part of the logical role. The Logical DBA role is usually independent of the Database software.
Application DBA	The Application DBA role deals with the Database from the table level and its related objects, and includes tasks such as: • Creates and loads tables, triggers, indices and other database objects. • Provides the data to be loaded into the Database and manages the data. • Requests certain changes to the Database (new userids, table changes). • Manages Application users of the Database (such as password) • Assists Physical DBA, as required, in repairing/resolving Databases Incidents. • Assists Physical DBA with the design of backup, recovery and archiving procedures and schedules. • Forecasts storage requirements (initiate changes accordingly). This responsibility is shared by the Application DBA and Physical DBA. • Shares performance monitoring and tuning of Database. The Application DBA is primarily responsible on the application level and the Physical DBA is primarily responsible in the physical level.
Physical DBA	The Physical DBA role deals with the Database as a whole up to and including the tablespaces, and includes tasks such as: • Installs, configures, upgrades and patches RDBMS and associated backup, restore, management and monitoring utilities and tools. • Starts and stops the Database and listener. • Monitors and maintains Database availability specified by the Application. • Daily restore/refresh of education/training Databases from baseline when required.

Term	Definition
	• Designs/develops backup/recovery/archiving procedures and schedules for Databases. • Debug, repairs, resolves Databases Incidents. Application DBA may assist with DB recovery as required. • Manages Database access control, creates, deletes and configures userids and groups according to Application owner. • Performs periodic Database storage reorganization including index and tablespace rebuilds. • Monitor, analyze and report Database storage capacity and utilization. • Creates Databases and associated objects up to and including the tablespaces. • Places tables in appropriate tablespaces as defined by the Application DBA. • Performs Application Release Management duties in Test and Production environment. Executes scripts and programs on behalf of Application DBA and developers to: o to drop/create/alter Database objects, o to load data into tables (process will be automated in the production environment), o to install new application releases. • Shares performance monitoring and tuning of Database duties with Application DBA. • Provides assistance in capacity planning based on growth and changes to the Databases. • Coordinates scheduled outages. • Monitors production Database performance statistics and maintains repository for these data. • Leads in resolution of infrastructure and Database software issues, liaises with vendors and Application DBA and developers to facilitate the remedial action. • Monitor, maintain and support Database replication (such as standby databases and Multi-Master Replication Databases). • Provide Disaster Recovery Service for Database. • Work with Application DBA and developers to perform Database stress testing. • Perform initial diagnostic activities to clarify root cause of application related Problems. • Monitor and respond to Database alert conditions and provide remedial action as needed. • Provide input to hardware, RDBMS and related software architecture changes.

APPENDIX B – REPORTS

Reports

- AES Hours used by account
    - Frequency: monthly
    - Format: Electronic
    - Recipient: Province (EHS)
- Database license usage
    - Frequency: monthly
    - Format: Electronic
    - Recipient: Province (EHS)
- Middleware license usage for products supported by EAS
    - Frequency: monthly
    - Format: Electronic
    - Recipient: Province (EHS)
- Billing report
    - Frequency: monthly
    - Recipient: Province (EHS)
- Other reporting will be described in the statements of work for services purchased by Clients and will be dependent upon the nature of the services

Alerts

- As requested by Clients

APPENDIX C – SYSTEMS

Intentionally Left Blank

APPENDIX D - SUPPORTED CUSTOMER LOCATIONS

Intentionally Left Blank

APPENDIX E - SERVICE PROVIDER SERVICE LOCATIONS

Intentionally Left Blank

APPENDIX F - AES SUPPORTED MIDDLEWARE

S. 15

S. 15

APPENDIX G – MIDDLEWARE SUPPORT

- Provide and maintain a current Client business/technical contact list for Middleware software.
- Supply Middleware and related utilities, tools software and all required licences. Province will maintain ownership of the software.
- Ensure Middleware version and release compatibility and specify maintenance level/patch requirements.
- Install/upgrade/patch/remove Middleware software and related utilities, tools.
- Provide Middleware environment and configuration requirements such as filesystem allocation and size, directory structures and host parameters.
- Create and configure Middleware environment (development, test, training/education and production) according to client specification
- Provide Middleware system-level security requirements such as groups, ownership ids.
- Create and manage Middleware system-level security according to Client specification.
- Provide Middleware object configuration requirements (such as number of MQ channels, queue manager, config file parameters, Websphere environment).
- Create, configure and manage Middleware objects and environments according to Client specification.
- Manage access to Middleware objects based on Client requests
- Perform Middleware log rotation, pruning and archiving.
- Configure Middleware utility and monitoring tool to perform tasks such as reporting, monitoring or alerting Middleware events (i.e. MQ channel stopped)
- Perform Middleware management and administrative tasks to support Application development and test teams.
- Work with Client to maintain Middleware production change window that meets their needs.
- Prepare and submit change requests.
- Approve Middleware Change Requests.
- Start/stop Middleware environment and Middleware objects.
- Monitor, report and optimize Middleware environment performance.
- Perform Middleware capacity planning, allocate storage and plan future growth based on Client requirements.
- Provide input on hardware and software changes that might affect Middleware environment.
- Perform system-level backup and recovery for Middleware environment.
- Report and provide information regarding Middleware system Problems.
- Troubleshoot, repair and resolve Middleware system software Problems.
- Contact Middleware vendor for technical support regarding software Problems.
- Validate Middleware software licensing compliance.

Managed Storage and Managed Backup Services

SOW 6

Table of Contents

Page

Table of Contents
(continued)

Page

1. SOW 6 - SCOPE AND SUMMARY

1.1 Definitions

Capitalized words used in this Statement of Work ("SOW") shall have the meanings given to such words in the Master Services Agreement. In the event that a term is not defined in the Master Services Agreement, it shall have the meaning provided in Appendix A of this SOW or in the body of this SOW.

1.2 Purpose of this Document

1.2.1 General

The purpose of this SOW is to describe the scope and functions of the Managed Storage Services and Managed Backup Services to be performed by Service Provider for the Province under the terms of the Agreement. This SOW sets forth the background and a general overview of the Managed Storage Services and Managed Backup Services in Section 1.3 (*Managed Storage Services and Managed Backup Services Overview*) below, and describes such services in greater detail in this SOW below using an outcomes-based approach.

The outcomes-based approach used to describe the services in Section 2 (*Managed Storage Services*), Section 3 (*Managed Backup Services*) and Section 4 (*Managed Storage Services and Managed Backup Services – Common Functions*) of this SOW is intended to allow Service Provider the ability to determine the most efficient manner of providing the Services so described while achieving all applicable SLAs or SLOs applicable to such Services; provided that in providing the Managed Storage Services and Managed Backup Services the Service Provider complies, at all times, with the Privacy Obligations, the requirements of the Security SOW and the Province's Policies, as applicable.

Accordingly, the specific procedures, processes and associated tasks, required to be undertaken by Service Provider to perform the Managed Storage Services and Managed Backup Services are not described in this SOW, but will be described more fully in the Managed Storage and Managed Backup Operating Manual (defined below). As a result, it is the intention of the Parties that Service Provider will do what is required to deliver the Managed Storage Services and Managed Backup Services in compliance with the requirements of this SOW, even though the specific procedures, processes and tasks to do so are not specifically identified or otherwise articulated in this SOW; provided that in doing so the Service Provider shall not be responsible for (or otherwise be required to undertake) those matters that are specified in this SOW as being the responsibility of the Province, a Client or a third party (where the third party is not a Subcontractor of Service Provider for purposes of providing Services under the Agreement).

1.2.2 Use RASIC Charts

Section 2 (*Managed Storage Services*), Section 3 (*Managed Backup Services*) and Section 4 (*Managed Storage Services and Managed Backup Services – Common Functions*) of this SOW include "RASIC" charts that describe the responsibilities of the Province and Service

Provider in respect of the Managed Storage Services and the Managed Backup Services. The "RASIC" charts are populated with "RASIC" indicators that are to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.2.3 Managed Storage and Managed Backup Operating Manual

For greater clarification, it is the intention of the Parties that the specific procedures, processes, tasks and functions not described in this SOW that are required to be performed by Service Provider in order to deliver the Managed Storage Services and the Managed Backup Services shall be described in detail in the operating manual (the "Managed Storage and Managed Backup Operating Manual"), to be prepared by Service Provider as part of the transformation activities under the Transformation SOW. The Managed Storage and Managed Backup Operating Manual shall form part of the Manual described in Section 4.8 of the Agreement.

The Parties acknowledge that on the Hand-Over Date, the Managed Storage and Managed Backup Operating Manual shall consist of the processes, procedures (and associated tasks and functions) that are in use by the Province immediately prior to the Hand-Over Date (the "Province Procedures") until the Province Procedures have been revised by Service Provider as contemplated in the Transformation SOW. The Parties acknowledge that the Province Procedures are in various states of completion and drafting, and will not necessarily articulate all processes, procedures, tasks and functions that will be required for Service Provider to provide the Managed Storage Services and the Managed Backup Services immediately following the Hand-Over Date.

1.2.4 Existing Service Locations, Transformation and Ownership

As of the Hand-Over Date, the hardware and software that comprises the existing storage and backup solution of the Province under this SOW are located at the Province Managed Storage Facilities, the Province Managed Backup Facilities and the Remote Application Server Locations and Remote Infrastructure Server Locations listed on Schedule 8 (Service Locations) of the Agreement. As part of the Transformation SOW, the Province Managed Storage Facilities and the Province Managed Backup Facilities will be replaced by the STMS Data Centres.

Regardless of the location of any Servers that are the subject of the Managed Storage Services or Managed Backup Services under this SOW, the Province Owned Equipment and all additions and upgrades thereto shall at all times be and continued to be owned by the Province, and the Service Provider Owned Equipment and all additions and upgrades thereto shall be and continue to be owned by Service Provider unless and until such Service Provider Owned Equipment is transferred to the Province in accordance with Article 28 (*Default and Termination*) of the Agreement.

1.2.5 Appendices

The following Appendices are attached to and form part of this SOW, whether or not they are specifically referred to in this SOW:

Appendix A – Defined Terms / Definitions

Appendix B – Reports

Appendix C – Systems
I. Hardware
II. Software

S15

Appendix E – Replication Bandwidth Requirements Evaluation Information Form

1.3 Managed Storage Services and Managed Backup Services Overview

Managed Storage Services

Managed Storage Services is the management of the storage of Data in storage tiers (Tier 1, Tier 2 and Tier 3) based upon performance and reliability required for such Data. The storage tiers are distinguished by the performance of the disk and the Storage Array (the amount of cache memory, speed and size of the disk and the size of the RAID group) and the reliability of the disk and the Storage Array (the type of Storage Array with its underlying redundancy components and the size of the RAID group). The Managed Storage Services establish the data storage foundation required to support the Province Data storage requirements. The Service Provider will use integrated Storage Hardware, Storage Software, and support solutions to provide the Managed Storage Services within the range of Data storage tiers identified, as appropriate.

From and after the Hand-Over Date and until the Managed Storage Services are transformed into the STMS Data Centres (in accordance with the Transformation SOW), the Service Provider will manage the existing storage infrastructure at, and perform the Managed Storage Services from, the Province Managed Storage Facilities. The Service Provider will perform the Managed Storage Services in support of the storage infrastructure located at the Province Managed Storage Facilities.

Managed Backup Services

Managed Backup Services is the management of the Backup and restoration of Data structured to meet requirements of accessibility, integrity, and recoverability (for example, basic tape-based Backup to disk-based Backup (VTL)). The Service Provider will use integrated Backup Hardware, Backup Software, and services to protect the Data.

From and after the Hand-Over Date and until the Managed Backup Services are transformed into the STMS Data Centres (in accordance with the Transformation SOW), the Service Provider will manage the existing tape based Backup infrastructure at, and

perform the Managed Storage Services from, the Province Managed Backup Facilities. The Service Provider will perform the Managed Backup Services in support of the existing tape based Backup infrastructure located at the Province Backup Facilities.

The Managed Backup Services delivered from the Province Managed Backup Facilities provides an integrated tape Backup and recovery solution for backing up and restoring Data that resides on Servers and Data that resides on the following workstations:

S15

Transformation of the Managed Storage and Managed Backup Services

The Service Provider will transform the Managed Storage Services and the Managed Backup Services as set forth in the Transformation SOW and thereafter, the Service Provider will perform the Managed Storage Services and the Managed Backup Services from the STMS Data Centres. The Managed Backup Services delivered from the STMS Data Centres provides a disk-based Backup service for full and incremental Backups of Data contained in Server primary storage. The Service Provider will perform the Managed Storage Services at the Province Managed Storage Facilities and the Managed Backup Services at the Province Managed Backup Facilities until the transformation activities set forth in the Transformation SOW are completed.

Diagram 1 below depicts the high level architecture of the Managed Storage Services and Managed Backup Services, post-transformation. Diagram 1 includes certain optional services that may be purchased by the Province.

S. 15

The Service Provider will be responsible for delivery of the following Managed Storage Services and Managed Backup Services, each of which is more fully described in this SOW:

Managed Storage Services

- Managed Storage Tier 1 Services
- Managed Storage Tier 1 Services with Replication Services (Optional Service)
- Managed Storage Tier 1 Services with Local Clone Services (Optional Service)
- Managed Storage Tier 2 and Tier 3 Services
- Storage Multi-Path Resilience Services
- Network Attached Storage (NAS) Services
- Managed RAM/SSD Services
- File System Archive Storage Services (Optional Service)

Managed Backup Services

- Managed Backup and Restore Services at Province Managed Backup Facilities
- Managed Backup and Restore Services at the STMS Data Centres

Managed Storage Services and Managed Backup Services - Common Functions

- Installation, Configuration and Testing Services - Province Managed Storage Facilities and Province Managed Backup Facilities
- Installation, Configuration and Testing Services – STMS Data Centres
- Service Delivery
- Connectivity Services

2. MANAGED STORAGE SERVICES

Managed Storage Services are comprised of three tiers of data storage listed below:

Managed Storage Tier 1 Services
Managed Storage Tier 2 Services
Managed Storage Tier 3 Services

The tiers above are distinguished by scalability, reliability and performance of the underlying Storage Hardware.

2.1 Managed Storage Tier 1 Services

Managed Storage Tier 1 Service is a class of disk storage that is the highest performing, highest availability and is designed with the most redundancy. The Managed Storage Tier 1 Service has additional redundancy through the incorporation of storage multipathing using Storage Multi-Path Resilience (see Section 2.5 below). Service Provider provides monitoring, configuration, control, and tuning software with continuous operational support for the Managed Storage Tier 1 Service.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Managed Storage Tier 1 Services	Responsibility	
Tasks and Functions	P	SP
Provide technical and operational monitoring and continuous support for the Storage Hardware and Storage Software in accordance with Change Management Process		R
Manage Storage Hardware and Storage Software maintenance requirements based on the manufacturer's recommended schedule (in addition, the Service Provider will manage third party Supplier relationships and conduct service-level reviews for Storage Hardware and Storage Software components provided in the scope of service)		R
Provide Performance Management, Capacity Management and load-balancing		R

Managed Storage Tier 1 Services	Responsibility	
Tasks and Functions	**P**	**SP**
services so that storage utilization is optimized across the Storage Hardware		
Connect Servers that require Managed Storage Services to the S. 15 S. 15 and assign storage to Servers that require Managed Storage Services		R
S15		R
Proactively manage the Storage Hardware, Storage Software and SAN infrastructure S. 15 and patch levels as documented in the then-current Supplier support matrix		R
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application(s) performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.2 Managed Storage Tier 1 with Replication Services (Optional Service)

Once both STMS Data Centres are Operational, the Province may purchase Managed Storage Tier 1 Services (described in 2.1 above) with Replication Services. Under the Managed Storage Tier 1 with Replication Services the Service Provider will move and Replicate the Province Data to a Service Provider Data Centre. S. 15

S. 15

S. 15 **Managed Storage Tier 1 Services with Replication Services lowers the time to restore operations as it relates to making Data available to a Server at the secondary Service Provider Data Centre. Managed Storage Tier**

1 Services with Replication Services provides for the creation of and enablement of Data content replication and Service Provider Data Centre site replication.

The Managed Storage Tier 1 Services with Replication Services may be ordered from the Services Catalogue by the Province and through placing a Service Request/Province Ordering System request in accordance with the Services Management SOW.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Managed Storage Tier 1 with Replication Services (Optional Service)	Responsibility	
Tasks and Functions	P	SP
Provide bandwidth requirements evaluation information requested by the Service Provider (in the form of the questionnaire attached as Appendix E) for the Server and Data targeted for Managed Storage Tier 1 with Replication Services	R	
Evaluate bandwidth requirements associated with the Data targeted for Managed Storage Tier 1 with Replication Services and the bandwidth requirement will be determined on a case by case basis.		R
Support operational processes to enable automated capacity adjustments and reallocation or reconfiguration to support Province Data replication		R
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application(s) performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.3 Managed Storage Tier 1 with Local Clone Services (Optional Service)

Once the STMS Data Centres are Operational, the Province may purchase Managed Storage Tier 1 Services (described in 2.1 above) with Local Clone Services. S. 15

S. 15

S. 15 **Managed Storage Tier 1 Services with Local Clone Services provides a copy of Province Data that can be managed by the primary Server or the management of the copy may be assigned to a second Server for Backup or testing purposes.**

The Managed Storage Tier 1 Services with Local Clone Services may be ordered from the Services Catalogue by the Province and through placing a Service Request/Province Ordering System request.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Managed Storage Tier 1 with Local Clone Services (Optional Service)	Responsibility	
Tasks and Functions	**P**	**SP**
Support operational processes to enable automated capacity adjustments and reallocation or reconfiguration to support a clone copy.		R
Create a Local Clone of the Province Data.		R
Provide Server-independent, online, real time data mirroring or mirroring at set intervals as defined by the Province.		R
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application(s) performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.4 Managed Storage Tier 2 and Tier 3 Services

Managed Storage Tier 2 Services is a class of disk storage that has medium performing, high availability and is designed with a high level of redundancy. The Managed Storage Tier 2 Services S. 15

S. 15

S. 15 **Service Provider provides monitoring, configuration, control, and tuning software with continuous operational support for the Managed Storage Tier 2 Services.**

Managed Storage Tier 3 Services is a class of disk storage that has an economy performing disk, lower availability than Managed Storage Tier 2 Services and is designed with a high level of redundancy. The Managed Storage Tier 3 Services S. 15

S. 15

S. 15 **Notwithstanding the foregoing, some of the Province Servers located in the Province Managed Storage Facilities, existing at the Hand-Over Date, that are tied to the Managed Storage Tier 3 Services will not have Storage Multi-Path Resilience. For greater certainty,** S. 15

S. 15 **Service Provider provides monitoring, configuration,**

control, and tuning software with continuous operational support for the Managed Storage Tier 3 Services.

Managed Storage Tier 2 and Tier 3 Services provides the Province with a leveraged, SAN based, storage platform.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Managed Storage Tier 2 and Tier 3 Services	Responsibility	
Tasks and Functions	**P**	**SP**
Manage Storage Hardware and Storage Software maintenance requirements based on the manufacturer's recommended schedule. Service Provider will manage Supplier relationships and conduct service-level reviews for Storage Hardware and Storage Software components provided in the scope of service.		R
Perform Performance Management, Capacity Management and load-balancing services so that storage utilization is optimized across the disk and channel infrastructure		R
Connect Servers that require Managed Storage Services to the S. 15 S. 15 and assign storage to Servers that require Managed Storage Services		R
S15		R
Proactively manage the Storage Hardware, Storage Software and SAN infrastructure S. 15 and patch levels as documented in the then-current Supplier support matrix.		R
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application(s) performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.5 Storage Multi-Path Resilience Services

Storage Multi-Path Resilience Services is the provisioning of additional performance and information availability enhancements for the Province's Servers by providing redundant paths for a Server to access storage Data so that it would take a multiple connectivity component failure (fault tolerance) to render a Server inaccessible to its associated storage. Designed for open server platforms connected to Service Provider SAN storage systems, Storage Multi-Path Resilience Services provides intelligent multi-path load balancing which allows channels to be utilized in the most efficient manner possible.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Storage Multi- Path Resilience Services	Responsibility	
Tasks and Responsibilities	P	SP
Provide integration of automatic load balancing allowing channels to share I/O workload		R
Provide automatic path failover to keep Data moving in the event of a HBA or SAN switch failure		R
Update and list all Servers, Server Type, and expected Gigabytes which the Server will have managed by Storage Multi-Path Resilience		R

2.6 Network Attached Storage (NAS) Services

Network Attached Storage (NAS) Services is file-level Server Data storage connected to an IP network providing data access to heterogeneous network clients. Network Attached Storage (NAS) devices located at the Province Managed Storage Facilities, existing at the Hand-Over Date, will be managed by the Service Provider from and after the Hand-Over Date. Network Attached Storage Service is the overall management of the Network Attached Storage (NAS), including monitoring, configuration, control, and tuning software, provided by the Service Provider.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Network Attached Storage (NAS) Services	Responsibility	
Tasks and Functions	P	SP
Perform Performance Management, Capacity Management so that storage utilization is optimized across the disk and channel infrastructure		R

Network Attached Storage (NAS) Services	Responsibility	
Tasks and Functions	P	SP
Manage the NAS Storage Hardware and Storage Software maintenance requirements based on the Supplier approved microcode and patch levels as documented in the then-current Supplier support matrix		R
Manage NAS Supplier relationships and review the level of service NAS Storage Hardware and Storage Software components		R
Proactively manage the Storage Hardware, Storage Software and NAS infrastructure to Supplier approved microcode and patch levels as documented in the then-current Supplier support matrix		R
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application(s) performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.7 Managed RAM/SSD Services

Managed RAM/SSD Services is solid state storage connected to a SAN providing Data access to Servers. RAM/SSD Storage devices located at the Province Managed Storage Facilities, existing at the Hand-Over Date, will be managed by the Service Provider from and after the Hand-Over Date. Managed RAM/SSD Services is the overall management of the RAM/SSD provided by the Service Provider. Support for Managed RAM/SSD Services is provided during business hours and on a commercially reasonable basis. In the event the Province requires any additional RAM/SSD Storage Software or RAM/SSD Storage Hardware in the delivery of the RAM/SSD Services, such additional RAM/SSD Storage Software or RAM/SSD Storage Hardware will be approved through the Change Order Process.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Managed RAM/SSD Services	Responsibility	
Tasks and Functions	P	SP
Manage the RAM/SSD Storage Hardware and RAM/SSD Storage Software maintenance requirements based on the Supplier approved microcode and patch levels as documented in the then-		R

Managed RAM/SSD Services	Responsibility	
Tasks and Functions	P	SP
current Supplier support matrix		
Manage RAM/SSD Supplier relationships and review the level of service RAM/SSD Storage Hardware and Storage Software components		R
Proactively manage the RAM/SSD Storage Hardware, RAM/SSD Storage Software and SAN connectivity infrastructure to Supplier approved microcode and patch levels as documented in the then-current Supplier support matrix		R
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.8 Archive Storage Repository Services (Optional Service)

Archive Storage Services is redundant hardware only solution that provides a primary content addressable system to store archive Data that is replicated to a secondary content addressable system for the purpose of extended Data protection against component or site failures but this is not the Disaster Recovery Site nor is it the disaster recovery solution. Archive Storage Repository Services are a prerequisite for File System Archive Storage Services.

Archive Storage Repository Services do not include Application specific archives (for example mail archive or database archive). Under the Archive Storage Repository Service, the Province is responsible for managing the Applications including how the Data is written to the archival storage allocation associated with the Applications, as well as the tools, processes, and people to define the archive policies and extract and retrieve Data where the Data is not covered under File System Archive Storage Services. Service Provider's obligation is limited to the provision of access to the designated hardware and allocating space on those devices where the Data is not covered under File System Archive Storage Services.

Archive Storage Repository Service Delivery	Responsibility	
Tasks and Functions	P	SP
Implement and configure the primary archive Storage Hardware at the Service Provider Data Centre and the secondary archive Storage Hardware		R

Archive Storage Repository Service Delivery	Responsibility	
Tasks and Functions	P	SP
at the Service Provider Data Centre (the STMS Interior Data Centre being the secondary storage system for the STMS Calgary Data Centre and the STMS Calgary Data Centre being the secondary storage system for the STMS Interior Data Centre) to manage and maintain the replicated Data		
Provide access to storage capacity on archive storage device(s) designated in Appendix C.		R
Allocate space on designated archive devices as requested by the Province through the Change Order Process		R
Provide notice (in writing or through minutes of joint Working Group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.9 File System Archive Storage Services (Optional Service)

Once the STMS Data Centres are Operational, the Province may purchase File System Archive Storage Services described in this Section 2.9. File System Archive Storage Services are comprised of components listed below:

- File System Archive Storage Services – Assessment
- File System Archive Storage Services – Installation
- File System Archive Storage Services – File Discovery
- File System Archive Storage Services – Service Delivery

File System Archive Storage Services ("FSA") is a service that provides automated file movement of S. 15

S. 15

If the Province elects to receive File System Archive Storage Services, then the Service Provider will establish, at the Services Provider's cost, a Proof of Concept ("POC") environment for the FSA to demonstrate that the File System Archive Storage Services

meet the Province's requirements. At such time the following will need to be agreed to by the Province and Service Provider prior to implementation of a POC:

- clearly defined POC evaluation/test criteria, including acceptance testing;
- timeline for the POC to be completed;
- Service Provider and Province resources assigned to work on the POC; and
- agreement of the Parties as to the successful completion of the POC (evaluation/test criteria are satisfied).

Upon the successful completion of the POC (the evaluation/test criteria are satisfied) the Province will purchase the File System Archive Storage Services in accordance with the provisions of this Section 2.9 and the Services Catalogue, as applicable.

2.9.1 File System Archive Storage Services - Assessment

File System Archive Storage Services - Assessment consists of a review of the Province Data to identify Province Data that may be a candidate for archiving under the File System Archive Storage Services prior to File System Archive Storage Services installation, configuration, integration, and testing. The main components of the File System Archive Storage Services pre-installation processes are as follows:

the first component of the pre-installation process is the Service Provider assessment of the Province's existing operating environment and the requirements of the Province contemplated for the File System Archive Storage Services;

the second component of the pre-installation process is the combined planning and design activities carried out by the Service Provider for determining the physical or logical requirements of the agreed to File System Archive Storage Services in accordance with the Province's requirements; and

upon completion of both the first and second components above, based on the collected and verified Data, the Service Provider will commence the installation, configuration, integration, and testing activities as further described in Sections 2.9.2 and 2.9.3 below.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

File System Archive Storage Services – Assessment	Responsibility	
Tasks and Functions	P	SP
Analyze the Province Data to determine the Data characteristics (such as file access times and file type)		R
Based upon the analysis above, the Service Provider will make recommendations to the Province for Data archive policies		R

File System Archive Storage Services – Assessment	Responsibility	
Tasks and Functions	P	SP
Determine the appropriate policies to implement based on the Service Provider recommendations and notify the Service Provider of such policies, in writing	R	
Configure the policies and directives for File System Archive Storage Services based on the Province approved recommendations above		R

2.9.2 File System Archive Storage Services - Installation

File System Archive Storage Services - Installation consists of the installation of the File System Archive-related Storage Hardware and Storage Software to support the File System Archive Storage Services.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

File System Archive Storage Services – Installation	Responsibility	
Tasks and Functions	P	SP
Install the Service Provider File System Archive Storage Services monitoring and management software agents to the Storage Hardware and Data file Servers		R

2.9.3 File System Archive Storage Services - File Discovery

File System Archive Storage Services - File Discovery is a Server-by-Server activity that: (i) analyzes and reports on file structures and (ii) reports on usage and/or access of the Province Data files.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

File System Archive Storage Services – File Discovery	Responsibility	
Tasks and Functions	P	SP
Provide the Service Provider access to load agents and run Scripts on each Server subscribing to the File System Archive Storage Services	R	

File System Archive Storage Services – File Discovery	Responsibility	
Tasks and Functions	P	SP
Identify and analyze the Province Data and storage usage characteristics in a defined Server (or group of Servers), using Service Provider supported file discovery Storage Software		R
Report to the Province, in writing, the Province's file usage patterns (this report is prepared once for each Server, at the time when File System Archive Storage Services are initiated for such Server)		R
Recommend to the Province certain policies for automated Data management of the Province's Data such as move, copy, and delete		R
Perform Performance Management and Capacity Management so that Storage Hardware utilization is optimized across the disk and channel infrastructure		R
Provide to the Province, on a monthly basis, standard system generated FSA reports as set out in Appendix B - Reports		R
Recommend to the Province, on an ongoing basis, the capacity and utilization requirements to ensure the Province has appropriate primary storage capacity to perform the Managed Storage Services (for example, manage the files stored on the primary storage by deleting files, moving files or archiving files or acquire additional storage capacity)		R
Maintain primary storage capacity in accordance with the recommendations above and where additional primary storage is required, order the same through the Province Ordering System, in accordance with the Services Management SOW	R	
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

2.9.4 File System Archive Storage Services – Service Delivery

The File System Archive Storage Services – Service Delivery consists of all services required to move the Province Data from primary storage (the Source File System) to File

System Archive Storage. File System Archive Storage Services automates file movement and retention through Province defined archive software policies and the mirroring of the archive Data within the same content addressable system. File System Archive Storage Services – Service Delivery is a redundant solution that replicates the Province's archive Data to a secondary content addressable system for the purpose of extended Data protection against component or site failures but this is not the Disaster Recovery Site nor is it the disaster recovery solution.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

File System Archive Storage Services – Service Delivery	Responsibility	
Tasks and Functions	P	SP
Define policies for automated Data movement and retention pursuant to the Province's retention specifications. Implementation of any policy changes is subject to the Change Order Process		R
Maintain Service Provider FSA system tools for automated transparent Data migration or archive activities from primary storage to archive repository		R
Provide the Province with access to migrated Province Data in the archived repository		R
Implement and maintain Service Provider security tools, policies, and practices for computer Data integrity (such as access codes, passwords and anti-virus programs) that are consistent with Province Policy and otherwise as defined in the Security Statement of Work in order to safeguard the Province's file Data in the possession of Service Provider against access by an unauthorized user		R
Provide a monthly utilization report on FSA Data storage, on a Server-by-Server basis as set out in Appendix - Reports B		R
Upon receipt of the defined Data migration and archive policies from Service Provider, review and approve such archive policies	R	
Provide notice (in writing or through minutes of Province/Service Provider joint working group meetings) of significant Client events that are out of the ordinary, where the Province is aware of such Client events (for example, increased storage requirements to meet a Client project, and Application performance testing that achieves higher levels of storage utilization than peak performance times) that may affect the Service Provider's provisioning of storage capacity or performance.	R	

3. MANAGED BACKUP SERVICES

Managed Backup Services is the protection of Data by creating a copy of such Data to allow for its recoverability in the event of destruction of the Data or loss or corruption of the primary copy of the Data and the Server. The Service Provider will perform available the Managed Backup Services for all Servers located at the Province Data Centres, Remote Application Server Locations and Remote Infrastructure Server Locations listed on Schedule 8 (*Service Locations*) of the Agreement. The Province will notify the Service Provider, in writing, of the specific Servers (at the locations identified above) and the Data that will receive Managed Backup Services. For clarity, S. 15

S. 15

S. 15 **Managed Backup Services are comprised of the following:**

- Managed Backup and Restore Services at Province Managed Backup Facilities
- Managed Backup and Restore Services at the STMS Data Centres
- VTL Backup Services with Replication to Secondary Site
- VTL Backup to Encrypted Offsite Tape
- Extended Retention Services

The Parties acknowledge and agree that the Province will obtain access and use rights with respect to the NetBackup Licences and such new licenses as required by Service Provider to perform the Managed Backup and Restore Services in accordance with the Change Order Process.

3.1 Managed Backup and Restore Services at Province Managed Backup Facilities

Managed Backup and Restore Services at Province Managed Backup Facilities provides tape based Backup and recovery services for the Servers located at the Province Data Centres, Remote Application Server Locations and Remote Infrastructure Server Locations listed on Schedule 8 (*Service Locations*) of the Agreement. S. 15

S. 15

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Managed Backup and Restore Services at Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP
Perform Backup administration responsibilities including, without limitation, installing and configuring all Backup Hardware and Backup		R

Managed Backup and Restore Services at Province Managed Backup Facilities	Responsibility	
Tasks and Functions	**P**	**SP**
Software and testing the Backup and restore processes, provision of all related equipment and supplies (including, for greater certainty, the supply of tapes) for Managed Servers		
Schedule Data Backups and Data Restore as required by the Province(scheduling includes designation of the timing of when Backups of Data are to be run, how frequently Backups of Data are to be run, how long Backup Data is to be retained) in accordance with the instructions provided by the Province. and monitor the completion of scheduled and on-demand Backup execution, for all Servers that require Managed Backup Services		R
Monitor the completion of scheduled and on-demand Backup and Restores for all Servers that require Managed Backup Services		R
Monitor and maintain the integrity of the Backup Application Catalogue on an ongoing basis		R
Monitor and manage active Data Backups and restores, during normal business hours, and respond to Incidents in accordance with Incident Management Process set forth in the Services Management SOW		R
Add, modify or remove a Server that requires Managed Backup Services in accordance with Change Management Process		R
Perform Performance Management and Capacity Management so that Backup utilization is optimized across the infrastructure		R
Add, modify and delete Backup configuration policies in accordance with Change Management Process		R
Notify the Province, in writing, of the Backup Client Software required for the Managed Backup and Restore Services at Province Managed Backup Facilities in order to meet the Province's desired Data Backup schedule, recovery time objectives and recovery point objectives		R
Maintain a current S. 15 count and provide to the Province as requested to support the license compliance and audit ability		R
Prepare and provide to the Province instructional guidelines for the installation of the appropriate Backup Client Software and associated Backup Hardware requirements of the Server		R

Managed Backup and Restore Services at Province Managed Backup Facilities	Responsibility	
Tasks and Functions	**P**	**SP**
Assist the Province with the configuration of Backup Client Software on Servers, other than the Service Provider Managed Servers, on a commercially reasonable basis		R
For Non-Managed Servers, the Service Provider will, at the request of the Province, provide the Province with Backup Client Software (on CD or other appropriate media) for installation on such Non-Managed Servers. For greater certainty, Backup Client Software under this section does not include non-Backup Supplier agents such as RMAN for Oracle		R
Validate that the Backup of Data to tape is executed to an offsite location such that the tape Backup and originating Data set, located on the primary Server, are not in the same physical location		R
Test the Service Provider Backup and restore processes and perform Backup and recovery for all Data that is to be backed up (this includes a restore test of a subset of Server Data as part of system acceptance), in accordance with the Change Management Process		R
Install and configure software components for Applications to interface with the Managed Backup Services (for example, database software or application-specific software) and ensure the integrity of the Data being backed up	R	
Assist the Province with installing and configuring software components for Applications to interface with the Managed Backup Services (for example, data base software or application-specific software)		R
Assist the Province's Application administrators in the configuring and testing of the Application Backup and restore processes		R
Notify the Service Provider, in writing, of the specific Servers (located at the Province Managed Storage Facilities, Province Managed Backup Facilities, Remote Application Server Locations and Remote Infrastructure Server Locations) and the Data that will receive Managed Backup Services	R	
If the Province fails to notify the Service Provider of the Data, on the Servers receiving Managed Backup Services, to be backed up, as a default the Service Provider will Backup all Data on such Servers		R

Managed Backup and Restore Services at Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP
For Legacy Servers that require additional Backup Hardware components, Backup Software or Application software in order for the Service Provider to provide Managed Backup Services to those Legacy Servers, the Province will be responsible for providing such Backup Hardware components or Backup Software as may be required to receive the Managed Backup Services (for example, Application software, Application Server software, or hardware enhancements such HBA cards or other features)	R	
Provide Exchange Tapes to the Province, upon request of the Province, using approved security procedures as defined in Security		R
Create Backup Application Catalogue CD for the Exchange Tapes master Server		R
Notify the Service Provider of: (a) unique tape handling or encryption requirements not otherwise addressed in this SOW; and (b) changes to the Province's requirements for Backup and tape storage, which will be addressed through the Change Management Process	R	
Encrypt Data written to Backup tapes, upon the request of the Province, subject to the technical limitations of the infrastructure at the Province Backup Facilities		R
Subject to provisions of the Security SOW, S. 15 S. 15 moved or transported outside of the Province Backup Facilities		R
Provide secure physical storage space at the Province Managed Backup Facilities for the storage of tapes used in connection with the performance of the Managed Backup Services	R	
Provide all robotic tape library handling and maintenance functions as required including, without limitation, cleaning tape drives, power cycling, ejecting jammed tapes and ensuring tape robot functionality		R

3.2 Managed Backup and Restore Services at the STMS Data Centres

3.2.1 VTL Backup Services with Replication to Secondary Site

VTL Backup Services with Replication to Secondary Site provides VTL based Backup and recovery services for the Servers located at the STMS Data Centres listed on Schedule 8 (*Service Locations*) of the Agreement, upon both such Data centres being Operational. The Service Provider will S. 15

S. 15

S. 15 **copied to the secondary VTL which is situated at the STMS Interior Data Centre.**

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

VTL Backup Services with Replication to Secondary Site	Responsibility	
Tasks and Responsibilities	P	SP
For Managed Servers, perform Backup administration responsibilities including, without limitation, installing and configuring all Backup Hardware and Backup Software and testing the Backup and restore processes, provision of all related equipment and supplies (including, for greater certainty, the supply of tapes)		R
Schedule Data Backups as required by the Province (scheduleing includes the designation of timing of when Backups of Data are to be run, how frequently Backups of Data are to be run, how long Backup Data is to be retained) in accordance with instructions provided by the Province		R
Monitor the completion of scheduled and on-demand VTL Backup and Restores for Servers designated by the Province to receive VTL Backup Services with Replication to Secondary Site		R
Monitor and maintain the integrity of the Backup Application Catalogue, on an ongoing basis		R
Monitor and manage active Data Backups and Restores, during normal business hours, and respond to incidents in accordance with Incident		R

VTL Backup Services with Replication to Secondary Site	Responsibility	
Tasks and Responsibilities	P	SP
Management Process		
Add, modify or remove a Server that requires Managed Backup Services in accordance with Change Management Process		R
Perform Performance Management and Capacity Management so that Backup utilization is optimized across the infrastructure		R
Add, modify and delete Backup configuration policies in accordance with Change Management Process		R
Notify the Province, in writing, of the Backup Client Software required for the VTL Backup Services with Replication to Secondary Site in order to meet the Province's desired Data Backup schedule, recovery time objectives, recovery point objectives		R
Maintain a current NetBackup license count and provide to the Province as requested to support the license compliance and audit ability		R
Prepare and provide to the Province instructional guidelines for the installation of the appropriate Backup Client Software and associated Backup Hardware requirements		R
Assist the Province with the configuration of Backup Client Software on Servers, other than the Service Provider Managed Servers, on a commercially reasonable basis.		R
For Non-Managed Servers, the Service Provider will, at the request of the Province, provide the Province with Backup Client Software (on CD or other appropriate media) for installation on such Non-Managed Servers. For greater certainty, Backup Client Software under this section does not include non-Backup Supplier agents such as S. 15		R
Test the Service Provider Backup and restore processes and perform Backup and recovery for all Data that is to be backed up (this includes a restore test of a subset of Server Data as part of system acceptance), in accordance with the Change Management Process		R
Install and configure software components for Applications to interface with the Managed Backup Services (for example, database software or application-specific software) and validate the integrity of the data being backed up.	R	

VTL Backup Services with Replication to Secondary Site	Responsibility	
Tasks and Responsibilities	P	SP
Assist the Province with installing and configuring software components for Applications to interface with the Managed Backup Services (for example, database software or application-specific software)		R
Assist the Province's Application administrators in the configuring and testing of the Application Backup and restore processes		R
Notify the Service Provider, in writing, of the specific Servers (located at the STMS Data Centres, Remote Application Server Locations and Remote Infrastructure Server Locations) and the Data that will receive Managed Backup Services	R	
If the Province fails to notify the Service Provider of the Data, on the Servers receiving Managed Backup Services, to be backed up, as a default the Service Provider will Backup all Data on such Servers		R
For Legacy Servers that require additional Storage Hardware components, Storage Software or Application software in order for the Service Provider to provide Managed Backup Services to those Legacy Servers, the Province will be responsible for providing such Storage Hardware components or Storage Software as may be required to receive the Managed Backup Services (for example, Application software, Application server software, or hardware enhancements such HBA cards or other features)..	R	
Notify the Service Provider of: (a) unique encryption requirements not otherwise addressed in this SOW; and (b) changes to the Province's requirements for Backup, which will be addressed through the Change Management Process	R	
Subject to the provisions of the Security SOW, encrypt all Data written to tapes prior to such tapes being moved or transported outside of the Province Backup Facilities		R

3.2.2 VTL Backup to Encrypted Offsite Tape Services

VTL Backup to Encrypted Offsite Tape Services is a VTL to tape based Backup and recovery service for the purpose of facilitating Backup and restore capabilities for Servers located in the STMS Data Centres, Remote Application Server Locations and Remote

Infrastructure Server Locations listed on Schedule 8 (*Service Locations*). S. 15

S. 15

S. 15

S. 15 **Once both the STMS Data Centres are Operational, the Province may continue to purchase VTL Backup to Encrypted Offsite Tape Services, as an economy service.**

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

VTL Backup to Encrypted Offsite Tape Services	Responsibility	
Tasks and Functions	P	SP
For Managed Servers, perform Backup administration responsibilities including, installing and configuring all Backup Hardware and Backup Software and testing the Backup and Restore processes, provision of all related equipment and supplies (including, for greater certainty, the supply of tapes)		R
Schedule Data Backups as required by the Province (the timing of when Backups of Data are to be run, how frequently Backups of Data are to be run, how long Backup Data is to be retained) and monitor the completion of scheduled and on-demand Backup execution		R
Monitor and maintain the integrity of the Backup Application Catalogue, on an ongoing basis		R
Monitor and maintain the robotic tape libraries		R
Provide desired Data Backup schedule, recovery time objectives, recovery point objectives, and Application information, in writing, through the Change Management Process	R	
Monitor and manage active Data Backups and Restores, during normal business hours, and respond to incidents in accordance with Incident Management Process		R
Add, modify or remove a Server that requires Managed Backup Services in accordance with the Change Management Process		R
Perform Performance Management and Capacity Management so that Backup utilization is optimized across the infrastructure		R

VTL Backup to Encrypted Offsite Tape Services	Responsibility	
Tasks and Functions	P	SP
Add, modify and delete Backup configuration policies in accordance with the Change Management Process		R
Notify the Province, in writing, of the Backup Client Software required for the VTL Backup to Encrypted Offsite Tape Services in order to meet the Province's desired Data Backup schedule, recovery time objectives and recovery point objectives		R
Maintain a current S. 15 count and provide to the Province as requested to support the license compliance and audit ability		R
Prepare and provide to the Province instructional guidelines for the installation of the appropriate Backup Client Software and associated Backup Hardware requirements		R
Assist the Province with the configuration of Backup Client Software on Servers, other than the Service Provider Managed Servers, on a commercially reasonable basis.		R
For Non-Managed Servers, at the request of the Province, provide the Province with Backup Client Software (on CD or other appropriate media) for installation on such Non-Managed Servers. For greater certainty, Backup Client Software under this section does not include non-Backup Supplier agents such as S. 15		R
Test the Service Provider Backup and Restore processes and perform Backup and recovery for all Data that is to be backed up (this includes a Restore test of a subset of Server Data as part of system acceptance), in accordance with the Change Management Process		R
Install and configure software components for Applications to interface with the Managed Backup Services (for example, database software or application-specific software)	R	
Assist the Province with installing and configuring software components for Applications to interface with the Managed Backup Services (for example, database software or application-specific software)		R
Test database Backup and restore functionality which consists of periodically testing database Backup and restore processes (creation, and maintenance of database scripting to support Backup efforts)	R	

VTL Backup to Encrypted Offsite Tape Services	Responsibility	
Tasks and Functions	P	SP
Assist the Province's Application administrators in the configuring and testing of the Application Backup and restore processes		R
Notify the Service Provider, in writing, of the specific Servers (located at the STMS Data Centres, Remote Application Server Locations and Remote Infrastructure Server Locations) and the Data that will receive Managed Backup Services	R	
If the Province fails to notify the Service Provider of the Data, on the Servers receiving Managed Backup Services, to be backed up, as a default the Service Provider will Backup all Data on such Servers		R
For Legacy Servers that require additional Storage Hardware components, Storage Software or Application software in order for the Service Provider to provide Managed Backup Services to those Legacy Servers, provide such Storage Hardware components or Storage Software as may be required to receive the Managed Backup Services (for example, Application software, Application Server Backup Software, or Backup Hardware enhancements such as HBA cards or other features)	R	
Notify the Service Provider of: (a) unique tape handling or encryption requirements not otherwise addressed in this SOW; and (b) changes to the Province's requirements for Backup and tape storage, both of which will be addressed through the Change Management Process	R	
S. 15 Data written to Backup tapes.		R
Provide off-site (to Server Data is being backed up from) S. 15 tape storage within a set of full and subsequent incremental versions.		R
Provide secure tape storage facilities exterior to the STMS Data Centres and provide tape librarian and handling services		R
Provide secure (bonded carrier) transportation of tapes to an offsite vaulting facility, as mutually agreed by the Parties		R
Provide all robotic tape library handling and maintenance functions as required including cleaning tape drives, power cycling, ejecting jammed tapes and ensuring tape robot functionality		R

3.2.3 Extended Retention Services

Extended Retention Services provides for the retention of Data on tape for a period of greater than ninety (90) days, for all of the Managed Backup Services.

For VTL Backup Services with Replication to Secondary Site (Section 3.2.1 above), the Province may request that the Data that is backed up be retained for a period of more than ninety (90) days (Extended Retention Services). S. 15

S. 15

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Extended Retention Services	Responsibility	
Tasks and Functions	P	SP
For Managed Servers, perform Backup administration responsibilities including installing and configuring all Backup Hardware and Backup Software and testing the Backup and restore processes, provision of all related equipment and supplies (including, for greater certainty, the supply of tapes)		R
Maintain a current S. 15 count and provide to the Province as requested to support the license compliance and audit ability		R
Encrypt all Data written to Backup tapes in STMS Data Centres		R
Notify the Service Provider of: (a) unique tape handling or encryption requirements not otherwise addressed in this SOW; and (b) changes to the Province's requirements for Backup and tape storage, which will be addressed through the Change Management Process	R	
Provide physical storage space at the at the STMS Data Centres for the storage of tapes used in connection with the performance of the Managed Backup Services (for greater certainty, S. 15 S. 15		R

Extended Retention Services	Responsibility	
Tasks and Functions	P	SP
S. 15		
Provide all robotic tape library handling and maintenance functions as required including cleaning tape drives, power cycling, ejecting jammed tapes and ensuring tape robot functionality		R

4. MANAGED STORAGE SERVICES AND MANAGED BACKUP SERVICES - COMMON FUNCTIONS

Managed Storage Services and Managed Backup Services - Common Functions (the "Common Functions") are services that are applicable to the Managed Storage Services set forth in Section 2 (*Managed Storage Services*) and the Managed Backup Services set forth in Section 3 (*Managed Backup Services*). The Common Functions are comprised of the following services to be provided by the Service Provider:

- Installation, Configuration and Testing Services – Province Managed Storage Facilities and Province Managed Backup Facilities
- Installation, Configuration, Integration and Testing – STMS Data Centres
- Service Delivery

4.1 Installation, Configuration and Testing Services - Province Managed Storage Facilities and Province Managed Backup Facilities

Installation, Configuration and Testing Services – Province Managed Storage Facilities and Province Managed Backup Facilities is the planning for any new Storage Hardware, Backup Hardware, Storage Software or Backup Software (due to hardware refresh or to support growth) in the Province Managed Storage Facilities or Province Managed Backup Facilities, and includes installation, configuration, integration and testing services for such new hardware and software. Using the Implementation Plan developed by the Service Provider, with support from the Province, the Service Provider will test and validate the connectivity and access to the Province Managed Storage Facilities and Province Managed Backup Facilities and test the agreed to services, including the storage and Backup equipment.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Installation, Configuration and Testing Services - Province Managed Storage Facilities and Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP

Installation, Configuration and Testing Services - Province Managed Storage Facilities and Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP
As of the Hand-Over Date, provide logical and physical access to Province Managed Storage Facilities and Province Managed Backup Facilities for the Service Provider to determine the requirements to support the introduction of new Storage Hardware, Backup Hardware, Storage Software or Backup Software for the Managed Storage Services and Managed Backup Services	R	
Identify the Storage Hardware, Backup Hardware, Storage Software or Backup Software requirements for any hardware refresh or to support growth at the Province Managed Storage Facilities and Province Managed Backup Facilities		R
Create the Implementation Plan (setting out the Service Provider's and the Province's responsibilities) for the ongoing installation, configuration, integration and testing of any new Storage Hardware, Backup Hardware, Storage Software or Backup Software to support the Managed Storage Services and Managed Backup Services. For clarity, the Implementation Plan will be subject to the Change Management Process		R
Provide all Storage Hardware, Backup Hardware, Storage Software or Backup Software (other than Province Retained Software) as required pursuant to the Implementation Plan		R
Provide project management services for the installation, configuration, integration and testing work to be performed in accordance with the Implementation Plan		R
Provide Storage Hardware, Backup Hardware, Storage Software or Backup Software Supplier relationship management (Supplier contract management)		R
Install all connectivity components to the Service Provider Demarcation Point (including, but not limited to, all fibre cabling and network connections from new Storage Hardware and Backup Hardware to the network switch ports (SAN switches and LAN switches)) or all Storage Hardware, Backup Hardware, Storage Software or Backup Software for connectivity to the Backup Servers located at the Province Managed Storage Facilities and Province Managed Backup Facilities (for greater certainty, the Service Provider will not be responsible to connect the existing or new SAN switches connected to the MAN as part of the SAN fabric extension)		R
Conduct a final review of the installation of new Storage Hardware, Backup Hardware, Storage Software or Backup Software (including Storage Arrays		R

Installation, Configuration and Testing Services - Province Managed Storage Facilities and Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP
and Backup Servers) to provide the Managed Storage Services and the Managed Backup Services, in accordance with the Implementation Plan		
Conduct testing as described in the Implementation Plan to validate the production readiness of new Storage Hardware, Backup Hardware, Storage Software or Backup Software (including storage arrays and Backup Servers)		R

4.2 Installation, Configuration, Integration and Testing - STMS Data Centres

Installation, Configuration, Integration and Testing – STMS Data Centres is the planning for any new Storage Hardware, Backup Hardware, Storage Software or Backup Software in the STMS Data Centres, and includes installation, configuration, integration and testing services for such new Storage Hardware, Backup Hardware, Storage Software or Backup Software.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Installation, Configuration, Integration and Testing – STMS Data Centres	Responsibility	
Tasks and Functions	P	SP
Identify the Storage Hardware, Backup Hardware, Storage Software or Backup Software requirements to support the Managed Storage Services and Managed Backup Services at the STMS Data Centres.		R
Create the Implementation Plan (setting out the Service Provider's and the Province's responsibilities) for the ongoing installation, configuration, integration and testing of any new Storage Hardware, Backup Hardware, Storage Software or Backup Software to support the STMS Data Centres, as such changes are agreed through the Change Management Process		R
Provide all Storage Hardware, Backup Hardware, Storage Software and Backup Software (other than Province Retained Software) as required pursuant to the Implementation Plan		R
Provide project management services for the installation, configuration, integration and testing work to be performed in accordance with the Implementation Plan		R
Provide Storage Hardware, Backup Hardware, Storage Software or Backup Software Supplier relationship management (Supplier contract		R

Installation, Configuration, Integration and Testing – STMS Data Centres	Responsibility	
Tasks and Functions	P	SP
management)		
Install and maintain all connectivity components required to connect to the Service Provider Demarcation Point (including, but not limited to, all fibre cabling and network connections from new Storage Hardware and Backup Hardware to the network switch ports (SAN switches and LAN switches)) or all Storage Hardware, Backup Hardware, Storage Software or Backup Software for connectivity to the Backup Servers located at the STMS Data Centres as required for the performance of the Services		R
Validate that the availability, bandwidth, latency and throughput of Service Provider WAN solution supports the requirements of the Managed Storage Services and the Managed Backup Service		R
Conduct a final review of the installation of new Storage Hardware, Backup Hardware, Storage Software or Backup Software (including storage arrays and Backup Servers) to provide the Managed Storage Services and the Managed Backup Services, in accordance with the Implementation Plan		R
Conduct testing as described in the Implementation Plan to validate the production readiness of new Storage Hardware, Backup Hardware, Storage Software or Backup Software (including Storage Arrays and Backup Servers)		R

4.3 Service Delivery

Service Delivery is the operational process required to maintain resource capacity, availability, continuity and committed service levels. Service Provider will provide the following recurring activities: patch management and Storage Hardware, Backup Hardware, Storage Software and Backup Software maintenance of Service Provider managed equipment; and the monitoring of such Storage Hardware, Backup Hardware, Storage Software and Backup Software or other recurring activities as agreed to in the Change Management Process.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Service Delivery	Responsibility	
Tasks and Functions	P	SP

Service Delivery	Responsibility	
Tasks and Functions	P	SP
Complete a managed storage or managed backup requirements definition request (Province Ordering System request) identifying services as defined in this Statement of Work required by the Province (for example, provisioning of additional storage, connectivity of additional Servers, or configuration changes)	R	
Respond to managed storage or managed backup requirements definition request (Province Ordering System request) to support requested changes to services identified in this Statement of Work including but not limited to provisioning of additional storage, connectivity of additional Servers, or configuration changes using the Change Management Process		R
Notify the Province in accordance with the provisions of the Services Management SOW in the event of a Problem impacting the Managed Storage Services or Managed Backup Services		R
Perform basic diagnostics in response to electronic alerts on Storage Hardware, Backup Hardware, Storage Software or Backup Software to verify proper functioning of such hardware and software to perform the Managed Storage Services and the Managed Backup Services		R
Proactively manage the Storage Hardware, Storage Software, Backup Hardware and Backup Software to Supplier approved microcode and patch levels as documented in the then-current Supplier support matrix		R
Monitor Storage Hardware, Backup Hardware, Storage Software and Backup Software to identify any Problems, failures, Data errors, or degradation in applicable Service Levels (as such Service Levels are set forth in Schedule 11 (Service Levels) to the Agreement), as well as improvements and expansion needs		R
In the event of degradation of the Managed Storage Services or the Managed Backup Services, will perform a root cause analysis to determine the cause of such degradation, and report the same to the Province, and take the appropriate action to restore the Services in the event such degradation		R
Update Managed Storage Services and Managed Backup Services Documentation to reflect changes (additions, modifications, deletions) in the physical and logical environment		R
Provide reports as defined in Appendix B to this SOW		R
Provide tape management services including tape ordering, cataloguing, tracking, loading, duplicating, managing scratch pool (ensuring there is		R

Service Delivery	Responsibility	
Tasks and Functions	P	SP
enough tapes in the tape library), tracking bad tapes and inventorying tapes for disposal, as required		
S. 15		R
	R	
Dispose of all Storage Hardware and Backup Hardware containing Data (for example, tapes, disk drives and memory) in accordance with Province Policy and the procedures set forth in the Service Management Statement of Work		R
For Province Managed Backup Facilities and Province Managed Storage Facilities, meet with the Province's Information and Communications Technology (ICT) Facilities Group on a weekly basis or ad hoc basis as may be necessary, for the purpose of ensuring that both Parties are aware of any issues that may impact the Province Managed Backup Facilities or Province Managed Storage Facilities or the Managed Backup Services or Managed Storage Services		R
For Province Managed Storage Facilities and Province Managed Backup Facilities, provide information to the Province's Information and Communications Technology (ICT) Facilities Group on a weekly basis or ad hoc basis, regarding facilities requirements to accommodate the refresh of Storage Hardware and Backup Hardware or growth (space/power/cooling requirements) in Province Managed Storage Facilities and Province Managed Backup Facilities, which will be subject to the Province's approval in accordance with the Change Management Process		R
Provide the Province a Backup Software license forecast annually		R
Provide all remote infrastructure management in Province Managed Storage Facilities and Province Managed Backup Facilities as require to perform the Services		R

4.4 Connectivity Services

Connectivity Services is the management of the connectivity equipment (such as switches, fibre cables) that connect Storage Arrays and Tape Libraries to Servers in such a way that

the Storage LUNs and Tape Drives appear as though they are directly attached to the Server. Connectivity Services are performed for the following:

- Connectivity Services in the Province Managed Backup Facilities or Province Managed Storage Facilities
- Connectivity Services – Service Provider Data Centre

4.4.1 Connectivity Services in the Province Managed Backup Facilities or Province Managed Storage Facilities

Service Provider will provide SAN connections for the Province's Servers to the Managed SAN Networks within the Province Managed Backup Facilities or Province Managed Storage Facilities.

Service Provider and the Province will perform the tasks and functions as indicated in the RASIC chart below.

Connectivity Services - Province Managed Storage Facilities and Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP
Monitor and manage the SAN Networks for the Managed Storage Services and Managed Backup Services		R
Provide SAN-attached connectivity from the Server to the Storage Arrays or Tape Libraries. For greater certainty, additional network communication requirements to the Application or Server (for example, IP, MAN, LAN, or WAN connectivity or network management services) are not included in the scope of Managed Storage Services and Managed Backup Services		R
Identify specific multipathing Storage software S. 15 S. 15 required for the Servers in connection with the Managed Storage Services and Managed Backup Services		R
For Legacy Servers that require additional Storage Hardware components, Backup Hardware components, Storage Software, Backup Software or Application software in order for the Service Provider to provide Connectivity Services to those Legacy Servers, the Province will be responsible for providing such hardware components or software as may be required to receive the Connectivity Services (for example, multipathing software or hardware enhancements such HBA cards or other features)	R	
Approve implementation of multipathing software on identified Servers as requested by Service Provider to perform the Connectivity Services on	R	

Connectivity Services – Province Managed Storage Facilities and Province Managed Backup Facilities	Responsibility	
Tasks and Functions	P	SP
Legacy Servers		
Install the required storage connectivity Storage Software or Storage Hardware for the Connectivity Services		R

4.4.2 Connectivity Services - Service Provider Data Centre

Service Provider will provide SAN connections for the Servers to the Managed SAN Networks within the STMS Data Centres.

Service Provider and the Province will have the responsibilities as indicated in the table below:

Connectivity Services – Service Provider Data Centre	Responsibility	
Tasks and Functions	P	SP
Monitor and manage the Managed SAN Networks for the Managed Storage Services and Managed Backup Services		R
Provide SAN-attached connectivity from the Server to the Storage Arrays or Tape Libraries		R
Identify specific multipathing Storage Software S. 15 S. 15 required for the Servers in connection with the Managed Storage Services and Managed Backup Services		R
Install the required storage connectivity Storage Software or Storage Hardware for the Connectivity Services		R

APPENDIX A –DEFINITIONS

APPENDIX A –DEFINITIONS

Definable Term	*Definition*
Agreement	means Master Services Agreement.
Application(s)	means the business applications developed and maintained by the Province Clients.
Archive Storage Repository Services	has the meaning given to it in Section 2.8 of this SOW.
Backup	means making a copy of Data so that the copy may be used to restore the original after a Data loss event.
Backup Application Catalogue	means the electronic database containing information on all backup jobs, tape and VTL information associated with a master backup Server.
Backup Client Software	means software residing on a Server for the purpose of Backup of Data.
Backup Hardware	means hardware required for the Managed Backup Services including, but not limited to, servers, tape libraries, tape drives, VTL, and the hardware listed in Appendix C.
Backup Software	means software required for the Managed Backup Services, including but not limited to the software listed in Appendix C .
Capacity Management	means the management of the capacity for the Managed Storage Services and Managed Backup Services to deliver such services to the Service Level Agreements
Change Management Process	has the meaning given to it in the Services Management SOW

Definable Term	*Definition*
Change Order Process	has the meaning given to it in Section 7.4 of the Agreement.
Client	has the meaning given to it in the Agreement and includes Broader Public Sector entities that buy storage and backup services directly from Workplace Technology Services.
Common Functions	has the meaning set forth in Section 4 of this SOW .
Configuration Item	means a component that needs to be managed in order to deliver the Managed Storage Services or Managed Backup Services consisting of hardware, software and documentation.
Connectivity Services	means the services described in Section 4.4 of this SOW.
Data	means the Province information in electronic format (for greater certainty, including Client information in electronic format).
DB Agents	means software required to interact between a database and the NetBackup application.
Data Base Administrator (DBA)	means a person who is responsible for the functional aspects of a database including: • recoverability - creating and testing Backups • integrity - verifying or helping to verify data integrity • security - defining and/or implementing access controls to the data • availability - ensuring maximum uptime • performance - ensuring maximum performance • development and testing support - helping programmers and engineers to efficiently utilize the database.
Disaster Recovery	has the meaning given to it in the Disaster Recovery SOW.
Disaster Recovery Site	has the meaning given to it in the Disaster Recovery SOW.
Exchange Tapes	means Data Backup tapes that contain the mail database Backups from the Province's Microsoft exchange servers.
Extended Retention Services	means the services described in Section 3.2.3 of this SOW.

Definable Term	*Definition*
File System Archive	means File System Archive Storage Services.
File System Archive Storage Services	means the services described in Section 2.9 of this SOW.
File System Archive Storage Services – File Discovery	means the services described in Section 2.9.3 of this SOW.
File System Archive Storage Services – Assessment	means the services described in Section 2.9.1 of this SOW.
File System Archive Storage Services – Installation	means the services described in Section 2.9.2 of this SOW.
File System Archive Storage Services – Service Delivery	means the services described in Section 2.9.4 of this SOW.
Host Bus Adapter (HBA)	means a device that connects a Host system to other network and storage devices.
Host	means a computer (typically a Server) connected to the network or SAN
Implementation Plan	means the project plan consisting of the steps required to deliver a technology project as part of Installation, Configuration and Testing Services.
Incident	has the meaning given to it in the Services Management SOW.
Input/Output (I/O)	means the communication between an information processing system (such as a computer, SAN or Storage Array), and another information processing system. Inputs are the signals or Data received by the system, and outputs are the signals or Data sent from it.
Installation, Configuration and Testing Services	means the services described in Sections 4.1 and 4.2 of this SOW.
Installation, Configuration and Testing Services – Province Managed Storage Facilities and Province Managed Backup Facilities	means the services described in Section 4.1 of this SOW.
Installation, Configuration, Integration and Testing – STMS Data Centres	means the services described in Section 4.2 of this SOW.
Internet Protocol (IP)	means a protocol used for communicating Data across a packet-switched internetwork using the internet protocol suite , known more completely

Definable Term	*Definition*
	in industry terms as "Transmission Control Protocol / Internet Protocol" ("TCP/IP")
Legacy Servers	means Province owned Servers.
Local Area Network (LAN)	means a computer network covering a confined geographic area such as a small building or small group of buildings in the same geographic location.
Local Clone	means an independently addressable copy of Data volume, that uses advanced mirroring technique for redundancy or business continuity purposes.
Logical Unit Number (LUN)	means a unique identifier used on a SCSI (Small Computer System Interface) bus that enables it to differentiate between up to eight separate devices (each of which is a logical unit); each LUN is a unique number that identifies a specific logical unit, which may be an end user, a file, or an application program.
Managed Backup and Restore Services at Province Managed Backup Facilities	means the services described in Section 3.1 of this SOW.
Managed Backup Services	means the services described in Section 3 of this SOW.
Managed RAM/SSD Services	means the services described in Section 2.7 of this SOW.
Managed SAN Networks	means the fibre channel network used for connectivity of Servers to Storage Arrays and Tape Libraries. For greater certainty this does not include the MAN connections between Province Managed Storage Facilities and Province Managed Backup Facilities.
Managed Servers	means Servers receiving Server Management Services under the Midrange SOW.
Managed Storage Services and Managed Backup Services - Common Functions or Common Functions	means the services described in Section 4 of this SOW.
Managed Storage Services	means the services described in Section 2 of this SOW.
Managed Storage Tier 1 with Replication Services (Optional Service)	means the services described in Section 2.2 of this SOW.
Managed Storage Tier 1 with Local Clone Service	means the services described in Section 2.3 of this SOW.

Definable Term	*Definition*
(Optional Service)	
Managed Storage Tier 1 Services	means the services described in Section 2.1 of this SOW.
Managed Storage Tier 2 Services	means the services described in Section 2.4 of this SOW.
Managed Storage Tier 2 and 3 Services	means the services described in Section 2.4 of this SOW.
Managed Storage Tier 3 Services	means the services described in Section 2.4 of this SOW.
Metropolitan Area Network (MAN)	means a large computer network that spans a metropolitan area (or is within a city) as its geographic scope falls between a WAN and LAN.
Mirror	means a complete logical representation of separate volume copies.
S. 15	S. 15
S. 15	S. 15 At issue for Inquiry
Network Attached Storage	means file-level computer Data storage connected to an IP network providing Data access to heterogeneous Servers.
Network Attached Storage (NAS) Services	means the services described in Section 2.6 of this SOW.
Non-Managed Servers	means Province Servers that are managed by a third party (other than the Service Provider).
Operational	means the STMS Data Centre Availability Date for each of the STMS Calgary Data Centre and the STMS Interior Data Centre as set forth in the Data Centre Services SOW.

Definable Term	*Definition*
Performance Management	means the management responsibility for day-to-day Capacity Management activities including monitoring, threshold detection, performance analysis and tuning, and implementing changes related to performance and capacity.
Proof of Concept	has the meaning given to it in Section 2.9 of this SOW.
Province Data Centres	means those listed on Schedule 8 (Service Locations) of the Agreement.
Province Managed Backup Facilities	means the following facilities where, at the Hand-Over Date, the Data Backup is carried out: S. 15 S. 15
Province Managed Storage Facilities	means the following facilities where, at the Hand-Over Date, the Data is stored: S. 15 S. 15
Province Ordering System	has the meaning given to it in the Services Management SOW.
RAM	means random access memory.
Redundant Array of Independent Disks (RAID)	means a technology that employs the simultaneous use of two or more hard disk drives to achieve greater levels of performance, reliability, and/or larger Data volume sizes.
Remote Application Server Locations	means those locations listed on Schedule 8 (Service Locations) of the Agreement.
Remote Infrastructure Server Locations	means those locations listed on Schedule 8 (Service Locations) of the Agreement.
Replication or Replicate	means the automated process of asynchronous duplication of information or Data so as to retain such information or Data in a secondary location
Restore	means the replacement of a file or files from Backup media.
SAN Media server	means a computer defined in NetBackup that has access to tape drives through SAN or network connection.
Server	means a Physical device distinguished by underlying operating system type and is connected to the LAN and in some cases the SAN.

Definable Term	*Definition*
Service Delivery	means the services described in Section 4.3.
STMS Data Centres	means the STMS Calgary Data Centre and the STMS Interior Data Centre and "STMS Data Centre" means either of them.
Service Provider Demarcation Point	has the meaning given to it in the Data Centre SOW.
Service Request	has the meaning given to it in the Services Management SOW.
Software	means software required for the Managed Storage Services and the Managed Backup Services, as the case may be.
Source File System	means the originating Data.
SSD	means solid state disk.
S. 15	
STMS Calgary Data Centre	has the meaning given to it in the Data Centre SOW.
STMS Interior Data Centre	has the meaning given to it in the Data Centre SOW.
Storage Multi-Path Resilience Services or Storage Multi-Path Resilience	means the services described in Section 2.5 of this SOW.
Storage Area Network (SAN)	means an architecture to attach remote computer storage devices (such as disk arrays, tape libraries, and optical jukeboxes) to Servers in such a way that the devices appear as locally attached to the operating system.
Storage Array	means a disk storage system which contains multiple disk drives. It is differentiated from a disk enclosure, in that an array has cache memory and advanced functionality including RAID protection.
Storage Equipment	means SAN and Storage Array hardware.
Storage Hardware	means hardware required for the Managed Storage Services including but not limited to, servers, disk storage and fibre channel switches, as more particularly described in Appendix C, as such appendix may be amended by agreement of the Parties.
Storage Software	means software required for the Managed Storage Services as more particularly described in Appendix C, as such appendix may be amended by agreement of the Parties.
Tape Drive	means a data storage device that reads and writes data stored on a magnetic tape.
Tape Library	means a storage device which contains one or more tape drives, a number of slots to hold tape cartridges, a barcode reader to identify tape cartridges and an automated method for loading tapes (a robot).
Testing	means an activity that verifies that a Configuration Item, IT Service, Process, or some other item or component meets its specification or agreed requirements.

Definable Term	*Definition*
Unstructured File Data	means data contained in files comprised of the natural-language text of documents or pictorial images not associated with Applications such as a database or email.
Virtual Tape	means a data storage virtualization technology that represents a backup tape on a storage component (usually hard disk storage).
Virtual Tape Library or VTL	means a data storage virtualization technology used typically for Backup and recovery purposes. A VTL presents a storage component (usually hard disk storage) as tape libraries or tape drives for use with existing Backup software.
VTL Backup Services with Replication to Secondary Site	means the services described in Section 3.2.1 of this SOW.
VTL Backup to Encrypted Offsite Tape Services	means the services described in Section 3.2.2 of this SOW.
Wide Area Network (WAN)	means a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).
WTS	means Workplace Technology Services.
Zone	S. 15

APPENDIX B - REPORTS

The Service Provider will provide to the Province the following reports at the times set forth in this Appendix B:

1. **Monthly Backup Report** – provided on a monthly basis on or before the 15th of each month;

2. **Monthly Retention Report** – provided on a monthly basis on or before the 15th of each month;

3. **Weekly Backup Success Report** - provided on a weekly basis, Monday a.m.; and

4. **Monthly Storage Report** - provided on a monthly basis on or before the 15th of each month.

Partial samples of the above noted reports are set forth below for example purposes only.

Monthly Backup Report

There will be one of these reports associated with each S. 15 master Server.

Current Month Backup Report		January
Server Name	KBs	Gigs
Server 1	52001888	49.59286499
Server 2	37103072	35.38424683
Server 9	185100305	176.5254068
Server 10	148530807	141.6500158
Server 11	80561410	76.82934761
Server 12	209684128	199.9703674
Server 13	74134262	70.69994164
Server 14	135210144	128.9464417
Server 15	118497689	113.0082026
Server 16	41421272	39.50240326
Server 17	53745679	51.25587368
Server 18	73891707	70.46862316
Server 19	7003680	6.679229736
Server 20	7080576	6.752563477
Server 21	122478016	116.8041382
Server 22	38879072	37.07797241
Server 23	298388448	284.5653992
Server 24	49958848	47.64447021
Server 25	5720938784	5455.912384
Server 26	71717920	68.39553833
Server 27	53195712	50.73138428
Server 28	132503083	126.3647871
Server 29	27745870	26.46052361
Server 30	238183710	227.1496868
Server 31	53230928	50.76496887
	8031187010	7659.136782

Monthly Retention Report

There will be one of these reports associated with each S. 15 master Server.

Server	Total GB
Server 1	6.88
Server 2	85.72
Server 3	66.33
Server 9	15.57
Server 10	16.49
Server 11	0
Server 12	0
Server 13	125.92
Server 14	328.75
Server 15	9.19
Server 16	97.16
Server 17	8.51
Server 18	187.85
Server 19	10.7
Server 20	156.41
Server 21	9.37
Server 22	9.3
Server 23	50.49
Server 24	9.81
Server 25	9.69
Server 26	65.3
Server 27	89.75
Server 28	8.65
Server 29	8.64
Server 30	8.57
Server 31	12.61

Total GB: 1397.66

Weekly Backup Success Report

There will be one of these reports associated with each NetBackup master Server.

		Total # Servers	19	19	19	19	19	19	19	Master
		# Backups not schedule	18	16	16	16	16	16	16	FULL Backup
		Total # Backups Run	1	3	3	3	3	3	3	Monthly Backup
		Successful Backups	1	3	3	3	3	3	3	No backup Scheduled
		Failures	0	0	0	0	0	0	0	Failed with Code
		% Success	100%	100%	100%	100%	100%	100%	100%	100.0%
		Nov-08	Sat	Sun	Mon	Tue	Wed	Thu	Fri	
	Client	S		1	2	3	4	5	6	7
S15	BUR	4	S15	OK	OK	OK	OK	OK	OK	OK
			catalog backup	OK		ok	ok	OK	OK	OK
			Jobs still Active/Pending	0	0	0	0	0	0	0
			Initials							
	BC		BC001		OK	OK	OK	OK	OK	OK
	BC		BC002		OK	OK	OK	OK	OK	OK
	BC		BC003	OK	OK	OK	OK	OK		OK
	BC		BC004	OK	OK	OK	OK	OK	OK	OK
	BC	1	BC005		OK	OK	OK	OK	OK	OK
S15	BC	1	BC006		OK	OK	OK	OK	OK	OK
	BC	1	BC007		OK	OK	OK	OK	OK	OK
	BC	1	BC008		OK	OK	OK	OK	OK	OK
	BC	1	BC009		OK	OK	OK	OK	OK	OK
	BC	1	BC010		OK	OK	OK	OK	OK	OK
	BC	1	BC011		OK	OK	OK	OK	OK	OK

Monthly Storage Report

There will be one of these reports associated with each Site.

S15																	
	MSS/Tier 3	No Application Defined	7	1,405.00	1,580.63	1,405.00	1,405.00	1,580.63	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2
	MSS/Tier 3		7	1,405.00	1,580.63	1,405.00	1,405.00	1,580.63	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2
	MSS/Tier 2	No Application Defined	99	5,314.48	6,099.39	5,314.48	5,314.48	6,099.39	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2
	MSS/Tier 2		99	5,314.48	6,099.39	5,314.48	5,314.48	6,099.39	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2
S15	-		106	6,719.48	7,680.02	6,719.48	6,719.48	7,680.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	4

Host Specific Metric

# Power/	Internal/	HostAccess	HostAccessibl	HostAccessi	Volume Group: Total (GB	Used (GI	Free (GB	Internal/JI	Array Total (GB)	Array Used (GB)	File System: Total (GB)	Used (GB)	Free (GB	Internal / JBO	ArrayTot	ArrayUs	Database: Total (G	Used (GI	Free (GB	Internal / JB	Array To	Array Used
0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

S15																	
	MSS/Tier 2	No Application Defined	13	252.00	289.60	252.00	252.00	289.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
	MSS/Tier 2		13	252.00	289.50	252.00	252.00	289.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
S15	-		13	252.00	289.50	252.00	252.00	289.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3

Host Specific Metric

# Power/	Internal/	HostAccess	HostAccessibl	HostAccessi	Volume Group: Total (GB	Used (GI	Free (GB	Internal/JI	Array Total (GB)	Array Used (GB)	File System: Total (GB)	Used (GB)	Free (GB	Internal / JBO	ArrayTot	ArrayUs	Database: Total (G	Used (GI	Free (GB	Internal / JB	Array To	Array Used
0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

S15																	
	MSS/Tier 2	No Application Defined	86	2,141.00	2,469.88	2,141.00	2,141.00	2,469.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
	MSS/Tier 2		86	2,141.00	2,469.88	2,141.00	2,141.00	2,469.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
S15			86	2,141.00	2,469.88	2,141.00	2,141.00	2,469.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3

Host Specific Metric

# Power/	Internal/	HostAccess	HostAccessibl	HostAccessi	Volume Group: Total (GB	Used (GI	Free (GB	Internal/JI	Array Total (GB)	Array Used (GB)	File System: Total (GB)	Used (GB)	Free (GB	Internal / JBO	ArrayTot	ArrayUs	Database: Total (G	Used (GI	Free (GB	Internal / JB	Array To	Array Used
0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

British Columbia\STMS Totals			1,162	58,442.01	66,824.67	########	58,442.01	66,824.67	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	71
British Columbia Totals			2,071	58,442.01	66,824.57	########	58,442.01	66,824.57	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	71
Grand Totals			1,162	58,442.01	66,824.57	96,294.37	58,442.01	66,824.57	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	71
Tier Totals																	
		No Application Defined	94	11,382.00	12,804.75	11,382.00	11,382.00	12,804.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2
	MSS/Tier 3		94	11,382.00	12,804.75	11,382.00	11,382.00	12,804.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
		No Application Defined	1,066	46,960.01	53,457.32	46,930.01	46,500.01	53,457.32	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
	MSS/Tier 2		1,066	46,930.01	53,457.32	46,960.01	46,960.01	53,457.32	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3
		No Application Defined	2	500.00	562.50	900.00	500.00	562.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2
	MSS/Tier 1		2	900.00	562.50	500.00	500.00	562.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	3

APPENDIX C - SYSTEMS

I. Hardware

1. Province Managed Storage Facilities and Province Managed Backup Facilities. The Storage Hardware and Backup Hardware for the Province Managed Storage Facilities and Province Managed Backup Facilities as of the Hand-Over Date is contained on the list provided by the Province to the Service Provider on March 26, 2009, which list has not been amended.

The Parties contemplates providing Managed Storage Tier 2 Services and Managed Storage Tier 3 Services using the CX3-80 Storage Hardware.

2. STMS Data Centres. The Storage Hardware and Backup Hardware contemplated for the STMS Data Centres is set forth in the table below. The Parties acknowledge that the table below addresses the baseline hardware architecture for Storage Hardware and Backup Hardware that the Service Provider will be implementing within the STMS Data Centres. The storage devices with the noted storage capacity and power consumption specifications will be the initial platforms from which storage services will be delivered.

Initial Service Provider Storage Hardware and Backup Hardware at STMS Data Centres

	Model	Raw GB	Power Consumption kVA
Tier 1	DMX4 120 R5 300GB	**21,000**	**10.15**
Tier 2	CX3-80 R5 400GB	**136,380**	**7.92**
Tier 3	CX3-40F R5 1000GB	**211,800**	**7.92**
SAN Switch	Cisco 9513 Switch	**na**	**6.74 per pair**
VTL	EDL - DL3D3000	**219,000**	**5.02**
Tape Silo	Tape Library; Sun SL8500, 10k slots,16 LTO4 drives		**Use average based on estimated load**
Tape Drives	Encrypted Tape drive T10kB Drives - bundled		**4.6**
NAS	NS20 INT-2DM-4GB-4 CU GIGE PORTS	**28,000**	**1.16**
Archive	DL3D 3000 config CX3-40 clone	**122,000**	**8.3**

II. Software

1. Province Managed Storage Facilities and Province Managed Backup Facilities. The Storage Software and Backup Hardware for the Province Managed Storage Facilities and Province Managed Backup Facilities as of the Hand-Over Date is set forth in the table below contained on the list provided by the Province to the Service Provider.

Third party	Software	Responsible for S/W
EMC	EMC ControlCenter Backup Advisor Active Engine S. 15 S. 15 S. 15 RTU S. 15 NAVI NAVI S. 15 NAVI Windows Software Utilities PPATH SYMM S. 15 SYMM S. 15 SMC S. 15 EMC CC S. 15 with S. 15 S. 15	Province
Sun	Solaris	Province
Symantec	S. 15	Province

2. STMS Data Centres. The Storage Hardware and Backup Hardware contemplated for the STMS Data Centres is set forth in the table below.

Third party	Software	Responsible for S/W
EMC	EMC ControlCenter Backup Advisor Active Engine S. 15 S. 15 NetBackup S. 15 RTU S. 15 NAVI NAVI S. 15 NAVI Windows Software Utilities PPATH SYMM S. 15 SYMM SECURE S. 15 SMC EMC S. 15 with S. 15 NEW S. 15	EDS
EMC	DiskXtender SRDF Point in Time	EDS
Sun	ACSLS server Key management server Solaris	EDS
Symantec	S. 15	Province
CA	CA Job Management S. 15 S. 15	EDS

Pages 620 through 621 redacted for the following reasons:
- -
S15, S15

APPENDIX E - REPLICATION BANDWIDTH REQUIREMENTS EVALUATION INFORMATION FORM

Configuration Information		
Specify Unidirectional or Bidirectional	Unidirectional ☐	Bidirectional ☐
Business Continuance Information		
Check Box for Data Migration Implementation	☐	
Data Transfer Metrics		
How much data will be transferred initially in GB		
How much data will be transferred incrementally in GB		
What time frame will incremental transfers occur? (24 hr clock)		
Copy Metrics (if applicable)		
How many hours to transfer initial?		
New Replication Solution		
What is the RPO? (In Minutes)		
What is the RTO? (In Minutes)		
Database Information		
List database vendor software and version	Vendor	Version
Is the database distributed or centralized?	Distributed ☐	Centralized ☐
Is the database OLTP or data warehouse?	OLTP ☐	Data Warehouse ☐
Database size (GB)?	Database growth rate (GB)?	

STMS Hosting Services

SOW ~~5A~~ - Service Management Services

TABLE OF CONTENTS

SOW X, Scope and Summary

1.1 Definitions

Capitalized words used in this Statement of Work ("**SOW**") shall incorporate the meanings given to such words in the Master Services Agreement (the "**Agreement**") and in the other SOWs (which form part of the Agreement), as applicable. For ease of reference, definitions of words set out in the Agreement which are key to the understanding of this SOW have been set out in Appendix A of this SOW. In the event that a term is not defined in the Master Services Agreement, it shall have the meaning provided in Appendix A of this SOW or in the body of this SOW.

1.2 Purpose of this SOW

The purpose of this SOW is to describe the scope and functions of the Service Management Services to be performed by Service Provider for the Province under the terms of the Agreement.

1.3 Appendices

The following Appendices are attached to and form part of this SOW, whether or not they are specifically referred to in this SOW:

APPENDIX A – DEFINITIONS - SERVICE MANAGEMENT SERVICES SOW
APPENDIX B – SERVICE MANAGEMENT REPORTING
APPENDIX C – SYSTEMS
APPENDIX D – SUPPORT CUSTOMER LOCATIONS
APPENDIX E – SERVICE PROVIDER SERVICE LOCATIONS
APPENDIX F – HARDWARE ASSET DATA ELEMENTS
APPENDIX G – SOFTWARE ASSET DATA ELEMENTS
APPENDIX H – CHANGE CATEGORIES AND LEAD TIMES
APPENDIX I – ASSESSMENT OF SEVERITY
APPENDIX J – PROVINCE CHANGE WINDOWS
APPENDIX K – CHANGE MANAGEMENT ENTRANCE CRITERIA
APPENDIX L – INCIDENT PRIORITIZATION MATRIX
APPENDIX M – SIGNIFICANT EVENT REVIEW
APPENDIX N – REQUEST LEAD TIMES
APPENDIX O – PROVINCE REPORTS
APPENDIX P – TIB GUIDELINES

1.4 Service Management Services Overview

The Service Management under this SOW provides a framework for managing operational activities that are undertaken to deliver the Services, and the interactions of Service Provider with the Province and its Client Organizations.

Subject to the provisions of Section 1.4.8 (*Outcomes Based Approach*), this SOW describes the scope of the following Service Management services to be provided pursuant to the terms of the Agreement:

(a) General Responsibilities;

(b) Billing;

(c) Asset Management;

(d) Change Management;

(e) Incident and Problem Management;

(f) Request Management;

(g) Service Management Overall Summary Reporting; and

(h) After Hours Service Desk (Optional Service).

1.4.1 General Responsibilities and Reporting Requirements

The General Responsibilities section of this SOW sets forth certain responsibilities of the Parties which apply to one or more other sections of this SOW, and sets out the reporting responsibilities of the Parties.

1.4.2 Asset Management

The following listed Asset Management Services are more particularly described in the following sections of this SOW:

(a) General Responsibilities;

(b) Province Owned Hardware Asset Management;

(c) Service Provider Owned Hardware Asset Management;

(d) Province Owned Software Asset Management; and

(e) Service Provider Owned Software Asset Management.

1.4.3 Change Management

The Change Management under this SOW facilitates the proper planning, analysis, communication, and scheduling of changes to hardware, software, and the Supported Infrastructure. Service Provider will use Province's Change Management Process and Province's Change Management Application in the delivery of the Services.

1.4.4 Incident and Problem Management

The Province and Service Provider, as the case may be, will provide the following Incident and Problem Management Services, as more particularly described in a following section of this SOW:

(a) Province:

- Level 1 Support for Incident Management;

(b) Service Provider:

- Level 2 and Level 3 Support for Incident Management;
- Problem Management; and
- Incident Management Interface.

1.4.5 Request Management

Service Provider will perform the following Request Management Services for the Province, as more particularly described in a following section of this SOW:

(a) receive, log, accept, route, monitor, fulfill, document and close Requests;

(b) receive Minor Service Requests entered by the Province Level 1 Support organization;

(c) receive Province Ordering System Requests;

(d) receive Requests by email from Authorized Requestors; and

(e) receive Major Changes or Requests and address them through the Request Management Process or the Change Order Process, as applicable.

1.4.6 After Hours Service Desk (Optional Service)

The After Hours Service Desk consists of receiving, logging and dispatching calls to the appropriate support team for Incidents received from the Province for all WTS services, excluding workstation services (which are redirected to the Province's Single Point of Contact for Workstations Services).

The After Hours Service Desk is an optional service that may be procured by the Province, at its discretion, through the Change Order Process.

1.4.7 Manual

For greater clarification, it is the intention of the Parties that the specific procedures, processes, tasks and functions not described in this SOW that are required to be performed by Service Provider in order to deliver the Services under this SOW shall be described in detail in the Manual, to be prepared by Service Provider as part of the transformation activities under the Transformation SOW. Service Provider will provide the Province with a copy of the Manual as updated by the Service Provider to account for material amendments, and at the request of the Province, from time to time.

The Parties acknowledge that following the Hand-Over Date, the Manual shall consist of the processes, procedures (and associated tasks and functions) that are in use by the Province immediately prior to the Hand-Over Date (the "**Province Procedures**") until the Province Procedures have been revised by Service Provider as contemplated in the Transformation SOW. The Parties acknowledge that the Province Procedures are in various states of completion and drafting, and will not necessarily articulate all processes, procedures, tasks and functions that will be required for Service Provider to provide the Services under this SOW immediately following the Hand-Over Date.

1.4.8 Outcomes Based Approach

The Services described in this SOW use an outcomes-based approach. The outcomes-based approach used to describe the services in this SOW is intended to allow Service Provider the ability to determine the most efficient manner of providing the Services so described while achieving all applicable Service Levels and performing all of the Service Provider's obligations; provided that in providing the Services under this SOW the Service Provider complies, at all times, with the Province's Change Management Process (and uses the Province's Change Management Application), and also complies with the Privacy Obligations, the requirements of the Security SOW and the Province Security Policies & Standards (as defined in the Security SOW).

Accordingly, the specific procedures, processes and associated tasks required to be undertaken by Service Provider to perform the Services under this SOW are not described in this SOW, but will be described more fully in the Manual. As a result, it is the intention of the Parties that Service Provider will do what is required to deliver the Services under this SOW in compliance with the requirements of this SOW, even though the specific procedures, processes and tasks to do so are not specifically identified or otherwise articulated in this SOW; provided that in doing so the Service Provider shall not be responsible for (or otherwise be required to undertake) those matters that are specified in this SOW or elsewhere in the Transaction Documents as being the responsibility of the Province, a Client Organization or a third party (where the third party is not a Subcontractor of Service Provider for purposes of providing Services under the Agreement).

1.5 Responsibility Charts

This SOW includes "Responsibility" charts that describe the responsibilities of the Province and Service Provider in respect of the Services described in this SOW, as indicated in the charts by an "R". The "R" is to be interpreted as follows:

> Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified.

1.6 Related SOWs

The following SOWs are important to the understanding of Service Management services set forth in this SOW:

- Transformation SOW
- Mainframe Management Services SOW

- Midrange Management Services SOW
- Storage and Backup Services SOW
- Security SOW
- Data Centre SOW
- Business Continuity and Disaster Recovery SOW

1.7 General Responsibilities

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

The Service Provider will provide the Province with electronic access to the Service Provider Service Desk Tool. Such access will in no way limit or restrict the Service Provider's responsibility to update the Province and the Province Service Desk Tool in respect of all Major Incidents and other related matters referred to in this SOW, nor will it in any way shift such responsibility from the Service Provider to the Province.

If there is a Province system that the Service Provider requires license rights or use rights to in order to perform the Services where such license or use rights are not otherwise provided to the Service Provider under the Transaction Documents (as defined in the Agreement), then the parties will address such access or license rights through the Change Management Process or the Change Order Process, as applicable.

General Responsibilities	Province	Service Provider
Authorization Matrix, Email Distribution & Escalation Paths		
Maintain and provide to Service Provider up to date Authorization Matrix for the following: (a) Asset Management; (b) Change Management; (c) Incident and Problem Management; (d) Request Management; and (e) Service Delivery Unit contacts for Province Ordering System Requests.	R	
Provide to Province written notification of updates to the Authorization Matrix identifying the Province and Client Organization Staff as soon as the Service Provider is made aware of such updates.		R
Establish, update and maintain Client Organization email distribution lists to be used for communications relating to Changes and Incidents, and provide updated distribution lists to Service Provider as soon as they are available.	R	

General Responsibilities	Province	Service Provider
Provide Province with documented updates to the Client Organization email distribution lists to be used for communications relating to Changes and Incidents as such changes become known to the Service Provider.		R
Provide documented communication procedures and escalation paths to the Service Provider to enable Service Provider to communicate with the Province when required to perform the Services.	R	
Provide documented escalation paths to the Province to enable Province to communicate with the Service Provider when required in connection with the daily operational matters related to the Services.		R
Communicate with the Province using the procedures and escalation paths provided by the Province from time to time to communicate with the Province when required to perform the Services.		R
Communicate with the Service Provider using the escalation paths provided by the Service Provider from time to time to communicate with the Service Provider when required in connection with the daily operational matters related to the Services.	R	
Communications		
Develop communication procedures for notifying the Province and Client Organizations of Minor Changes and Minor Incidents, in consultation with the Province, and include such procedures in the Manual.		R
Consult with the Service Provider and provide input to the communication procedures developed by the Service Provider for notifying the Province and Client Organizations of Minor Changes and Minor Incidents.	R	
Communicate with Province and Client Organizations regarding Minor Changes and Minor Incidents in accordance with the Change communication procedures set out in the Manual which are developed in consultation with the Province.		R
Access and User Licensing Rights		
Provide Service Provider Personnel with access and user-licensing rights to use and access the following, as required by Service Provider to perform the Services:	R	

General Responsibilities	Province	Service Provider
(a) the Province's Change Management Application; (b) the Province's Incident Management Application; (c) the Province's Problem Management Application; and (d) the Province Ordering System, as may be reasonably required, to Service Provider Personnel who have been designated by Service Provider for purposes of providing the Services.		
Provide to the CSC and Province (EHS) Staff web-based access (and appropriate license rights for 40 members of the Province Staff) to Service Provider Service Desk Tool for access to the Service Provider Incidents.		R
Provide to the Service Provider Personnel access to the Province Service Desk Tool and appropriate license rights for 100 concurrent users jointly between the Province and the Service Provider.	R	
Training		
Provide to Service Provider Personnel initial "train-the-trainer" training and subsequent "train-the-trainer" training with respect to major releases of the following (being a release that includes functionality changes or changes in the manner in which the following is used): (a) the Province's Change Management Application; (b) the Province's Incident Management Application; (c) the Province's Problem Management Application; and (d) the Province Ordering System. The training may be instructor lead or may be provided online (computer based), as determined by the Province. Province shall supply training facilities for any instructor lead training.	R	
Attend the initial "train-the-trainer" training and subsequent "train-the-trainer" training with respect to major releases of the following (being a release that includes functionality changes or changes in the manner in which the following is used), as provided by the Province: (a) the Province's Change Management Application; (b) the Province's Incident Management Application; (c) the Province's Problem Management Application;		R

General Responsibilities	Province	Service Provider
and (d) the Province Ordering System. Service Provider will be responsible for any travel and living costs for Service Provider Personnel to attend such training.		
Provide to Service Provider Personnel documented updates to procedures relating to the following and respond to inquiries from the Service Provider's trainers regarding such updates: (a) the Province's Change Management Process and Change Management Application; (b) the Province's Incident Management Application and processes; (c) the Province's Problem Management Application and processes; and (d) the Province Ordering System and related documentation.	R	
Provide ongoing user-training, as may be necessary, to Service Provider Personnel on the operation of the following: (a) Province's Change Management Processes and Change Management Application; (b) Province's Incident Management processes and Incident Management Application; (c) Province's Problem Management processes and Problem Management Application and (d) Province Ordering System processes and the Province Ordering System. Service Provider shall supply training facilities for such training and will be responsible for any travel and living costs for Service Provider Personnel to attend such training.		R
Provide to Province Staff initial "train-the-trainer" training and subsequent "train-the-trainer" training with respect to major releases of the Service Provider Service Desk Tool (being a release that includes functionality changes or changes in the manner in which the following is used). The training may be instructor lead or provided online (computer based), as determined by the Service Provider. Service Provider shall supply training facilities for any instructor lead training.		R
Attend the initial "train-the-trainer" training and subsequent	R	

General Responsibilities	Province	Service Provider
"train-the-trainer" training with respect to major releases of the Service Provider Service Desk Tool (being a release that includes functionality changes or changes in the manner in which the following is used). Province will be responsible for any travel and living costs for Province Staff to attend such training session.		
Provide to Province Staff documented updates to procedures relating to the Service Provider Service Desk Tool and respond to inquiries from the Province's trainers regarding such updates.		R
Provide ongoing user-training, as may be necessary, to Province Staff with respect to the operation of the Service Provider Service Desk Tool. Province shall supply training facilities for such training and will be responsible for any travel and living costs for Province Staff to attend such training.	R	
Review, maintain, update and provide to the Province, as soon as they become available, the updated Service Provider Service Desk Tool documentation.		R
Review, maintain, update and provide to the Service Provider, as soon as they become available, the updated Province Service Desk Tool documentation.	R	
ITIL Framework		
Comply with the ITIL framework for Incident Management, Problem Management and Change Management.	R	
Comply with the ITIL framework for Incident Management, Problem Management and Change Management.		R
Reporting		
Produce and provide to Province reports identified in *Appendix B – Service Management Reporting*, and any other reporting required to be provided by the Service Provider as provided elsewhere in this SOW or in the Transaction Documents (as defined in the Agreement).		R
Make available to the Service Provider reports from the Province Service Desk Tool for Change Management and Incident related reports which are required for the Service Provider to perform the Services, which reports are set forth in *Appendix O – Province Reports*.	R	

1.8 Billing

The Service Provider will invoice the Province for the Services provided in accordance with the provisions of the Agreement. The Parties acknowledge that the invoices will initially be manually generated, but that the data to be input into the invoices will be auto-mated upon the completion of the Billing Module as contemplated in the Transformation SOW.

Billing	Province	Service Provider
Issue manually generated invoices for the Services in accordance with the Agreement until the Billing Module (as defined in the Transformation SOW) is completed (which is expected at month 7, being October, 2009), at which time the Service Provider will invoice the Province for the Services using the Billing Module.		R

1.9 Asset Management

Asset Management consists of the management of the data related to Hardware Assets and Software Assets, throughout their lifecycles. The components of Asset Management are:

(a) Province Owned Hardware Asset Management;

(b) Service Provider Owned Hardware Asset Management;

(c) Province Owned Software Asset Management; and

(d) Service Provider Owned Software Asset Management.

1.9.1 Asset Management - General Responsibilities

The *Asset Management – General Responsibilities* section of this SOW sets out the general responsibilities of Service Provider and the Province with respect to the management of the Hardware Assets and the Software Assets used to provide the Services.

The Province will provide the Service Provider with a list of the Hardware Assets and the Software Assets in existence as of the Hand-Over Date, containing data elements set out in *Appendix F – Hardware Asset Data Elements* and in *Appendix G – Software Asset Data Elements* (collectively, the "**Data Elements**") to the extent that such Data Elements are readily available to or otherwise recorded by the Province (the "**Initial Hardware List**" and the "**Initial Software List**" respectively). The parties acknowledge that the Initial Hardware List and the Initial Software List may not be complete or accurate, and will not include all of the Data Elements. To the extent that the Service Provider becomes aware, in the ordinary course of providing the Services, of any additional Hardware Assets, Software Assets or Data Elements that should have been included in the Initial Hardware List or the Initial Software List, then the Service Provider shall update the respective lists with such information. To the extent that the Province becomes aware of any additional Hardware Assets, Software Assets or Data Elements

that should have been included in the Initial Hardware List or the Initial Software List, including any Hardware Assets and Software Assets that are purchased by the Province after the Hand-Over Date that form part of the Supported Infrastructure, then the Province shall provide such information to the Service Provider as soon as possible.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Asset Management General Responsibilities	Province	Service Provider
Upon the occurrence of an internal reorganization or other similar internal reassignment within the Province that result in changes to Client Organization codes attached to the Hardware Assets and Software Assets, provide the Service Provider with information regarding the particulars of the resulting changes to the Client Organization codes and names as soon as possible. To the extent possible, provide the Service Provider with the Hardware Assets and Software Assets information generated from the Province Ordering System and the CAS Install Base (as the same may be updated by the Province as a result of the internal reorganization or other similar internal reassignment), to assist the Service Provider in updating the Hardware Asset and Software Asset information required to be maintained by Service Provider.	R	
Produce and make available monthly reports listing Hardware Assets and Software Assets categorized by Client Organization code or Client Organization name, and the Province Ordering System asset tag, as more particularly described in *Appendix B – Service Management Reporting*		R
Report to Province on a quarterly basis regarding any non-compliance to the hardware and software currency standards set out in the Annual Operating Plan, indicating where such non-compliance exists at the request of the Client Organization.		R
Designate an individual who will act as the point of contact on behalf of the Service Provider and who will have the authority to inform the Province regarding non-compliance to hardware and software currency standards. Inform Province of this individual's identity and position and supply to Province any other relevant information necessary to communicate with this individual.		R
Designate an individual who will act as the point of contact on behalf of the Province and who will have the authority to resolve non-compliance to hardware and software currency standards. Inform Service Provider of this individual's identity and position and supply to Service Provider any other relevant information	R	

Asset Management General Responsibilities	Province	Service Provider
necessary to communicate with this individual.		

1.9.2 Province Owned Hardware Asset Management

The *Province Owned Hardware Asset Management* section of this SOW sets out the responsibilities of the Service Provider and the Province with respect to the management of the inventory of Province Owned Hardware Assets.

The level of detail regarding the Hardware Assets is identified in *Appendix F – Hardware Asset Data Elements* (see Section 1.9.1 above regarding the Initial Hardware List).

The activities described in this section are transitory since all Province Owned Hardware Assets will be retired and eventually replaced with Service Provider Owned Hardware Assets.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Province Owned Hardware Asset Management	Province	Service Provider
Provide the Initial Hardware List to Service Provider within 10 Business Days of the Hand-Over Date.	R	
Track and record the Province Owned Hardware Assets that are used to provide the Services in accordance with the data elements set out in *Appendix F – Hardware Asset Data Elements*, as well as the asset tags used in the Province Ordering System (to the extent known by the Service Provider), starting with the Initial Hardware List. The list of Province Owned Hardware Assets shall be categorized by Client Organization code or Client Organization name.		R
Maintain and update Province Owned Hardware Asset information in the Initial Hardware List as required, and provide updated information to the Province commencing on the 7th month following the Hand-Over Date (being October 2009), in an electronic format as and when updates are made (for sharing with Client Organizations as the Province determines). The electronic format shall initially consist of a CSV file, but may be in such other electronic format as the parties may mutually agree in writing through the Change Management Process or through Governance, both acting reasonably.		R
Track the date and time for delivery, installation, relocation, upgrades, retirement and disposal of Province Owned Hardware Assets on the Initial Hardware List, as updated by the Service		R

Province Owned Hardware Asset Management	Province	Service Provider
Provider.		
Provide Service Provider with copies of known maintenance agreements on the Hand-Over Date, to the extent available, and the client codes and other relevant information required for Service Provider to exercise the Use Rights for the maintenance agreements, for the Province Owned Hardware Assets.	R	
Maintain and monitor the schedule of expirations of known maintenance agreements relating to the Province Owned Hardware Assets.		R
Provide to the Province notification of expiration of maintenance agreements relating to Province Owned Hardware Assets, at least three months but not more than six months prior to expiration of a maintenance agreement.		R
Update documented processes and procedures set out in the Manual, as may be required, in order to support compliance with maintenance agreements with third party hardware suppliers for Province Owned Hardware Assets.		R
Comply with the Use Rights for the maintenance agreements with third party hardware suppliers, as set out in the Master Transfer Agreement.		R

1.9.3 Service Provider Owned Hardware Asset Management

The *Service Provider Owned Hardware Asset Management* section of this SOW sets out the responsibilities of the Service Provider with respect to the management of the inventory of Service Provider Owned Hardware Assets.

The level of detail regarding the Hardware Assets is identified in *Appendix F – Hardware Asset Data Elements*.

Service Provider will perform the tasks or functions as indicated in the table below.

Service Provider Owned Hardware Asset Management	Province	Service Provider
Track and record the Service Provider Owned Hardware Assets that are used to provide the Services in accordance with the data elements set out in *Appendix F – Hardware Asset Data Elements*, as well as the asset tags used in the Province Ordering System. The list of Service Provider Owned Hardware Assets shall be categorized by Client Organization code or Client Organization name.		R

Service Provider Owned Hardware Asset Management	Province	Service Provider
Maintain and update Service Provider Owned Hardware Asset information as required, and provide updated information to the Province on a monthly basis in an electronic format as and when updates are made (for sharing with Client Organizations as the Province determines). The electronic format shall initially consist of a CSV file, but may be in such other electronic format as the parties may mutually agree in writing through the Change Management Process or through Governance, both acting reasonably.		R
Track the date and time for delivery, installation, relocation, upgrades and retirement and disposal of Service Provider Owned Hardware Assets.		R
Maintain and monitor the schedule of expirations of leases of Service Provider Owned Hardware Assets that are used to provide the Services and renew the leases where required.		R
Maintain and monitor the schedule of expirations of maintenance agreements relating to the Service Provider Owned Hardware Assets and renew the maintenance agreements where required.		R
Update documented processes and procedures set out in the Manual, as may be required, in order to support compliance with maintenance agreements with third party hardware suppliers for Service Provider Owned Hardware Assets.		R

1.9.4 Province Owned Software Asset Management

The *Province Owned Software Asset Management* section of this SOW sets out the responsibilities of the Service Provider and the Province with respect to the management of the inventory of Province Owned Software residing on Hardware Assets managed by Service Provider (see Section 1.9.1 above regarding the Initial Software List).

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Province Owned Software Asset Management	Province	Service Provider
Provide Initial Software List to Service Provider within 10 Business Days of the Hand-Over Date.	R	
Track and record the Province Owned Software Assets that are used to provide the Services in accordance with the data elements set out in *Appendix G – Software Asset Data Elements*, as well as the asset tags used in the Province Ordering System (to the extent known by the Service Provider), starting with the Initial Software List. The list		R

Province Owned Software Asset Management	Province	Service Provider
of Province Owned Software Assets shall be categorized by Client Organization code or Client Organization name.		
Maintain and update Province Owned Software Asset information in the Initial Software List as required, and provide updated information to the Province in an electronic format as and when updates are made (for sharing with Client Organizations as the Province determines), commencing on the 7th month following the Hand-Over Date (being October 2009). The electronic format shall initially consist of a CSV file, but may be in such other electronic format as the parties may mutually agree in writing through the Change Management Process or through Governance, both acting reasonably.		R
Maintain and monitor the third party software licenses, maintenance agreements, and software support agreements during the first 6 months following the Hand-Over Date in the same manner as previously maintained and monitored by the Province prior to the Hand-Over Date. Maintain and monitor the schedules of expirations of third party software licenses, maintenance agreements, and software support agreements using Service Provider processes commencing on the 7th month following the Hand-Over Date (being October 2009).		R
Provide to Service Provider, on the Hand-Over Date, all relevant information regarding compliance with third party software licenses, software maintenance agreements, and software support agreements required by the Service Provider for compliance with the Use Rights.	R	
Maintain the Access Rights Contracts and the Province Maintenance Agreements as required under the Master Transfer Agreement.	R	
Comply with the Use Rights for the third party software licenses, maintenance agreements, and software support agreements as contemplated in the Master Transfer Agreement.		R
Update processes and procedures in the Manual, as may be required, to support compliance with third party software licenses, maintenance agreements, and software support agreements, commencing on the 7th month following the Hand-Over Date (being October 2009).		R

1.9.5 Service Provider Owned Software Asset Management

The *Province Owned Software Asset Management* section of this SOW sets out the responsibilities of the Service Provider and the Province with respect to the management of the inventory of Service Provider Owned Software residing on Hardware Assets managed by Service Provider.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Service Provider Owned Software Asset Management	Province	Service Provider
Maintain and monitor the schedule of expirations of software licenses and maintenance service contracts for Service Provider Owned Software.		R
Provide all relevant information to the Province regarding the Province's compliance requirements with third party software supplier agreements for Service Provider Owned Software.		R
Manage compliance with third party software supplier licenses and agreements for Service Provider Owned Software.		R
Comply with third party software supplier licenses and agreements for Service Provider Owned Software.	R	

1.9.6 Asset Disposal

The responsibilities of the Parties for the disposal of Assets forming part of the Supported Infrastructure is set forth in the Data Centre Services SOW.

1.10 Change Management

Change Management consists of facilitating the proper planning, analysis, communication, and scheduling of Changes to the Supported Infrastructure. A Change that will amend the scope of the Services will be addressed through the Change Order Process set out in the Agreement.

The purpose of Change Management is to utilize standardized methods and procedures for efficient and prompt handling of Changes and RFCs in order to minimize Problems and Incidents.

By October 2009, the Province will provide the Service Provider with a complete listing of the network configuration elements (consisting of routers, ports, switches, MAC addresses, IP addresses and fully qualified domain names) for all of the Province's servers that form part of the Supported Infrastructure as of the Hand-Over Date so that, in the event of a network router/switch Change, the Service Provider will have the required information necessary to bring any impacted servers back online. The Service Provider will be responsible for managing such

network configuration information (once received from the Province) as changes are made for the Service Provider's own use in providing the Services.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Change Management	Province	Service Provider
Request for Change (RFC) and Change Management		
Comply with and implement Changes in accordance with the Province's Change Management Process and use the Province Change Management Application.		R
All Service Delivery Units will comply with the Province's Change Management Process and use the Province Change Management Application.	R	
Submit RFCs through the Province's Change Management Application for Changes to be implemented by Service Provider in compliance with the lead times specified in *Appendix H – Change Categories and Lead Times*.		R
Include the Incident number from the Province Service Desk Tool in the RFC where the RFC is required to resolve an Incident or where the RFC causes an Incident.		R
Provide technical details regarding the impact, backout effort, and assessment of risk on the Service Provider, the Province and Service Delivery Units for all RFCs submitted by the Service Provider through the Province's Change Management Application, in accordance with the guidelines set out in *Appendix I - Assessment of Severity*.		R
Obtain the necessary approvals as required under the Province's Change Management Process and the Authorization Matrix prior to the implementation of a Change. The approvals will require Client Organization approvals and Province (EHS) approvals as specified in the Authorization Matrix for dedicated and shared services, and the approval of the Change Management Coordinator for RFCs processed through the Province's Change Management Application.		R
Provide to Service Provider the approval of RFCs pursuant to the Authorization Matrix and establish standing approvals for Standard RFCs, in each case where determined appropriate by the Province, and within the lead times specified in *Appendix H – Change Categories and Lead Times*.	R	
Approve or disapprove all Changes related to the provision of		R

Change Management	Province	Service Provider
the Services in accordance with the Province's Change Management Process and within the lead times specified in *Appendix H – Change Categories and Lead Times*.		
Provide to Service Provider, to the extent the Province is able prior to their implementation, and in any event as soon as reasonably practicable, information regarding RFCs to which the Service Provider is not a party that may impact the provision of the Services (the "**Out-of-Scope RFCs**").	R	
Provide to Province, to the extent the Service Provider is able prior to their implementation, and in any event as soon as reasonably practicable, the potential risks and adverse impacts (and where known the actual impacts) of the Out-of-Scope RFCs on the provision of the Services.		R
Notify both the Change Management Coordinator and the appropriate individuals identified in the Authorization Matrix of the potential risks and adverse impacts to the Province and Client Organizations, as applicable, regarding any proposed RFC, to the extent known or reasonably foreseeable to the Service Provider.		R
Consult with Service Provider regarding the potential impact of a proposed Change as it relates to the provision of the Services.	R	
Prioritize or resolve conflicts (1) among Out-of-Scope RFCs and RFCs issued by Service Provider, and (2) any other RFCs that impede or restrict the Service Provider from performing the Services as contemplated under the Agreement.	R	
Prioritize and manage the RFCs that are approved and entered into in the ordinary course of providing the Services (and for greater clarification, this excludes the RFCs that are prioritized by the Province as set forth immediately above), and comply with the standards for the priority of RFCs attached as *Appendix H – Change Categories and Lead Times* and the RFC priorities established by the Province as contemplated above.		R
Update all Service Provider RFCs through the Province's Change Management Application (within three hours of implementation where technically possible) with information regarding all progress that occurs consisting of any actions taken to correct issues.		R
Update all Service Provider RFCs through the Province's Change Management Application with information regarding any associated Incidents which have occurred as a result of the		R

Change Management	Province	Service Provider
implementation of a Change, as soon as reasonably possible once such Incidents become known to Service Provider.		
Implement duly approved in-scope RFCs following the Province's Change Management Process and in accordance with the procedures for implementation described in the Manual.		R
Coordinate with Service Provider the preparation, testing and implementation of Out-of-Scope RFCs that may impact provision of the Services.	R	
Coordinate with Province the preparation, testing and implementation of Out-of-Scope RFCs that may impact provision of the Services.		R
Review and analyse records of Changes and RFCs to identify and determine existence of any operational trends of a negative or problematic nature and recurring Problems, and advise the Province of the results on an ongoing basis but not less than quarterly.		R
At the request of the Province from time to time, provide recommendations to the Province for the rectification of recurring Problems and trends of an adverse or problematic nature, in consultation with the Province and any relevant Service Delivery Units.		R
Emergency Changes and Authorization Matrix		
Implement Emergency Changes as set out in *Appendix H – Change Categories and Lead Times.*		R
Change Windows and Freeze Periods		
Utilize established Change Windows set out in *Appendix J – Province Change Windows* for scheduling and implementing Changes that may cause an outage, degradation or adverse impact on the provision of the Services.		R
Remain available on a standby (on-call) basis and assist the Client Organization with Services, during the Client Organization's application change windows, as may be requested by the Client Organization through the Province Ordering System or by way of an RFC, as applicable. All such requests will be made pursuant to a draw down account established between the Client Organization and the Service Provider.		R

Change Management	Province	Service Provider
Provide to Service Provider Change Freeze Period requirements for Client Organizations or WTS.	R	
Comply with Province Change Freeze periods.		R
Change Management Meetings		
Schedule, chair and participate with Service Delivery Units, Client Organizations and Service Provider in weekly Change Management meetings that are specific to matters relating to and held during the Fire Season, and provide reasonable notification to Service Provider of such meetings.	R	
Participate with Province, Service Delivery Units and Client Organizations in weekly Change Management meetings that are specific to matters relating to and held during the Fire Season, as scheduled and chaired by the Province and reasonably notified to the Service Provider (which may be on short notice in the case of live fires).		R
Schedule, chair and participate in Change Management meetings (which may be weekly or at other frequencies determined by the Province, and may be held as separate meetings for different subject matters and purposes), which are other than for the Fire Season, and provide reasonable notice to the Service Provider of those meetings which Service Provider is to attend, for purposes of the following: (a) reviewing the RFCs with Province Technical Peer Review groups or at the management level (as determined by the Province); (b) consideration of the impact of the RFCs and Out-of-Scope RFCs before implementation (where possible) and required coordination among the impacted parties; (c) consideration and review of TIBs; and (d) such other purposes as determined necessary by either the Province or the Service Provider.	R	
Participate in Change Management meetings scheduled and chaired by the Province and notified to the Service Provider (which may be weekly or at other frequencies determined by the Province, and may be held as separate meetings for different subject matters and purposes), which are other than for the Fire Season, for purposes of the following:		R

Change Management	Province	Service Provider
(a) reviewing the RFCs with Province Technical Peer Review groups or at the management level (as determined by the Province); (b) consideration of the impact of the RFCs and Out-of-Scope RFCs before implementation (where possible) and required coordination among the impacted parties; (c) consideration and review of TIBs; and (d) such other purposes as determined necessary by either the Province or the Service Provider.		
Schedule, chair and participate in meetings with the Change Coordination Entities to review, coordinate and approve specific RFCs that will impact more than one Service Delivery Unit and the Services (which may be weekly or at other frequencies determined necessary by the Province), and provide the Service Provider with reasonable notice of those meetings which Service Provider is to attend.	R	
Review Out-of-Scope RFCs in the Province Change Management Application, and the reports made available to Service Provider set forth in *Appendix O – Province Reports* to assess the impacts on the Services and discuss them the Province at the Change Management meetings.		R
Participate in meetings of Change Coordination Entities that relate to the Services, as notified by the Province to the Service Provider.		R
RFCs – Testing, Closure and Reviews		
Perform sufficient testing, based on the technical nature of the proposed Change, both before and after the implementation of the Change, and confirm the existence of an appropriate backout plan.		R
Design, implement and test LOB Applications not managed by the Service Provider (such as exchange and blackberry applications), as determined necessary by the Province following Service Provider implemented Changes to the Supported Infrastructure.	R	
Once the Service Provider completes implementation and updates comments in the RFC, review implementation comments and close RFC in Province's Change Management	R	

Change Management	Province	Service Provider
Application.		
Respond to and participate in any review reasonably requested by the Province in respect of a Change where no Incident was reported, using the Significant Event Review process in accordance with *Appendix M – Significant Event Review*.		R
Upon email or oral request from Province, respond to Province inquiries regarding Changes.		R
Make Service Delivery Unit representatives available for issue determination discussions with the Province and Service Provider following an Incident resulting from an Out-of-Scope RFC.	R	
TIBS and Communications		
Make TIBs available to Service Provider and provide Service Provider Personnel with access to the Province's TIB application.	R	
Provide Province with Service Provider Personnel contact information to be added to the Province's TIB application, and provide the Province with applicable updates from time to time as changes are made to such Service Provider Personnel contact information.		R
Produce TIBs regarding Major Changes using the Province TIB application, for review and acceptance by the Province and dissemination to Client Organizations through the Province's TIB application. Comply with the guidelines set forth in *Appendix P - TIB Guidelines*, for purposes of producing TIBs for the Province.		R
Prepare Service Bulletins based upon the TIBS regarding a Major Change, and provide to Province for review and acceptance by the Province prior to dissemination to Client Organizations.		R
Disseminate approved Service Bulletins prepared by Service Provider regarding a Major Change to Client Organizations.	R	

1.11 Incident and Problem Management

The *Incident and Problem Management* section of this SOW describes the responsibilities of the Service Provider and the Province relating to Incident and Problem Management services.

1.11.1 General Responsibilities for Incident & Problem Management

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

General Responsibilities: Incident & Problem Management	Province	Service Provider
Assignment Group Information		
Provide the Province with Assignment Group information, including all updates made by Service Provider from time to time, to facilitate the appropriate assignment of Incidents by Province to the Service Provider.		R
Upon changing a Service Provider Assignment Group, provide to Province relevant information with respect to the change.		R
Enter Service Provider Assignment group information into the Province Service Desk Tool, and all updates to such information as soon as practicable following receipt of the updates from the Service Provider.	R	
CSC Documentation		
Make available to the CSC the operational documentation containing up-to-date information for each Server consisting of the Assignment Group, the Service Provider's primary, secondary and tertiary support contact information, the Service Provider escalation contact, and the Client Organization contact (as such Client Organization information becomes known to the Service Provider in accordance with the provisions in Section 1.7 above), so that the CSC can triage, assign and escalate Incidents as required.		R
Incidents and Resolution		
Include the RFC number from the Province Service Desk Tool in the Incident where the Incident is resolved by an RFC or where the RFC causes the Incident.		R
Monitor and escalate Incident tickets in the Incident Management Application in accordance with the CSC Online Procedures.	R	
Track the Incident to resolution (which resolution may occur at the Level 2 or Level 3 Support) and close Incidents in the Province's Incident Management Application for Incidents that have been resolved.	R	
Provide the Service Provider with a documented process (as determined by the Province) to transfer Incidents (and related	R	

General Responsibilities: Incident & Problem Management	Province	Service Provider
information) that are unrelated to the Services from Service Provider to the CSC for Incidents.		
Comply with the process provided by the Province to transfer Incidents (and related information) that are unrelated to the Services from Service Provider to the CSC.		R
Provide to Province CSC updates to scripts and processes relating to resolutions determined by Service Provider for previously resolved Incidents and Known Errors, as they become known to Service Provider from time to time.		R
Update CSC scripts and processes relating to resolutions determined by Service Provider for previously resolved Incidents and Known Errors, as provided by Service Provider to CSC.	R	
Status Communications		
Provide status information to the Client Organization Contact, as requested by the Client Organization, to keep Client Organization informed of progress of the resolution of the Incident.	R	
Provide status and progress information to the Client Organization Contact, if requested by the Client Organization, to keep Client Organization informed of progress of the resolution of the Incident.		R
Communicate with Client Organizations regarding occurrence of a Major Incident.	R	
Unrelated Incidents		
Perform Incident Management for Incidents that are not within the scope of the Services.	R	
Notify Service Provider (through the Province's communication tool) of Major Incidents not within the scope of the Services that impact or could be reasonably expected to impact the ability of the Service Provider to provide the Services.	R	
Provide the Province with Service Provider Personnel contact information to be added to the Province's communication tool for purposes of receiving notices of Major Incidents not within the scope of the Services which could impact the ability of the Service Provider to provide the Services.		R
Significant Event Review Process		
Conduct Significant Event Review process for Incidents, in	R	

General Responsibilities: Incident & Problem Management	Province	Service Provider
accordance with *Appendix M – Significant Event Review*, including making personnel from WTS and Province Partners available for Significant Event Reviews.		
Respond to and participate in any meetings for WTS Significant Event Reviews of Incidents relating to or otherwise impacting the Services when requested to do so by the Province upon reasonable notice. Refer to *Appendix M – Significant Event Review*.		R
Provide written input (which may be by email) for WTS Significant Event Reviews of Incidents as requested by the Province within five (5) Business Days of receiving the email or written request from the Province. Refer to *Appendix M – Significant Event Review*.		R
Respond to and participate in short conference calls / meetings (which may be called on short notice) among the Province and other Service Delivery Units to troubleshoot active high priority operational issues or Incidents relating to or otherwise impacting the Services, when requested to do so by the Province.		R

1.11.2 Incident Management

Incident Management is intended to restore normal service operation to a service as quickly as possible and to minimize the adverse impact of an Incident on operations. Incident Management manages the lifecycle of all Incidents.

The CSC will provide the first point of contact (Level 1 Support) to Client Organizations. The CSC will provide communication channels and an escalation path for Incidents among Client Organizations, WTS, Province Partners and the Service Provider.

Service Provider will supplement the CSC by providing Level 2 Support and Level 3 Support. Upon receipt of an Incident for the Services, Service Provider will initiate Incident Management as applicable for the designated support level.

Incident Management provided outside of Business Hours is offered by the Service Provider to the Province as an optional service. Refer to the section 1.13 in this SOW which is entitled *After Hours Service Desk (Optional Service)* for a description of this optional service.

1.11.3 Incident Management – Province

The objective of the Province CSC is to provide Level 1 Support to Client Organizations. The CSC acts as a filter that allows calls to pass through to Level 2 and Level 3 Support when it is necessary. The CSC will be the primary point of contact used by the Service Provider to communicate the status of Incidents and to notify the Province of any Major Incidents (Priority 1

and 2 Incidents) detected by the Service Provider. The CSC will also be the point of contact used by the Service Provider to assign Incidents to other Service Delivery Units.

The Province will perform the tasks or functions as indicated in the table below.

Level 1 Support	Province	Service Provider
CSC and Level 1 Support		
Provide a single point of entry through the CSC for receiving and recording all Incidents.	R	
With respect to calls or messages received during CSC Hours of Operation, provide Level 1 Support consisting of the following: (a) filter and classify reported Incidents and create a ticket for the Incident in the Incident Management Application; (b) receive and deal with inquiries or complaints; (c) redirect Minor Service Requests to Service Provider using the Request Management Process; (d) provide initial Problem determination based upon the CSC Online Procedures; (e) resolve Incidents where possible when previously determined work-around solutions are available (first call resolutions); (f) route Incidents not related to the Services to other appropriate Assignment Groups for resolution; and (g) assign Incidents related to the Services to the Service Provider Level 2 Support, where not resolved at the Level 1 Support.	R	

1.11.4 Incident Management – Service Provider

The *Incident Management – Service Provider* section of this SOW describes the responsibilities relating to Incident Management services and Level 2 and Level 3 Support provided by the Service Provider.

Service Provider will perform the tasks or functions as indicated in the table below.

Level 2 & Level 3 Support	Province	Service Provider
Validate that the Incidents assigned to Service Provider by Province are related to the Services, and reassign the Incidents to the CSC that are not related to the Services using the process		R

Level 2 & Level 3 Support	Province	Service Provider
provided by the Province (see Section 1.11.1 above).		
Assign a Service Provider Assignment Group member to each Incident and manage, update and resolve the Incidents related to the Services.		R
Produce, verify and implement the resolution of the Incidents assigned to the Service Provider, and where a resolution is not readily available, provide and implement a Work-around solution as a temporary measure.		R
Verify successful resolution of the Incident with Client Organization Contact.		R
Update Incidents in accordance with the CSC Procedures and through the Province's Incident Management Application with information regarding all progress that occurs regarding the Incident (consisting of any actions taken to resolve the Incident), and information regarding any outages related to the Incident (including the length and time of the outage).		R
Determine whether any Incidents relating to the Services are duplications of any other Incidents, and notify the CSC of any such duplication.		R
Determine the sequence for resolving Incidents based upon the priorities defined in *Appendix L – Incident Prioritization Matrix.*		R
Determine whether the Incident is a Major Incident as set out in *Appendix L – Incident Prioritization Matrix*, and notify the CSC of all such Major Incidents at the time such determination is made.		R
Review and analyse records of previously resolved Incidents and Known Errors to identify and determine if a defined method of resolution exists and is available to be implemented, and notify the CSC of the particulars of all such available resolutions.		R
Consult with Client Organization Contact to determine a course of action for restoring normal business operations following the occurrence of an Incident, and work with Client Organization to restore normal business operations within the scope of the Services.		R
Monitor the status of all Incidents assigned to Service Provider Assignment Group until Service is restored or the Incident is resolved, and communicate such status to the Contact of the Client Organization impacted by the Incident.		R
Submit RFCs , as may be necessary, to restore the Service, and where it is not practicable to submit RFCs in advance, record		R

Level 2 & Level 3 Support	Province	Service Provider
corrective actions taken after the Service has been restored, and in each case in accordance with the Province's Change Management Process.		

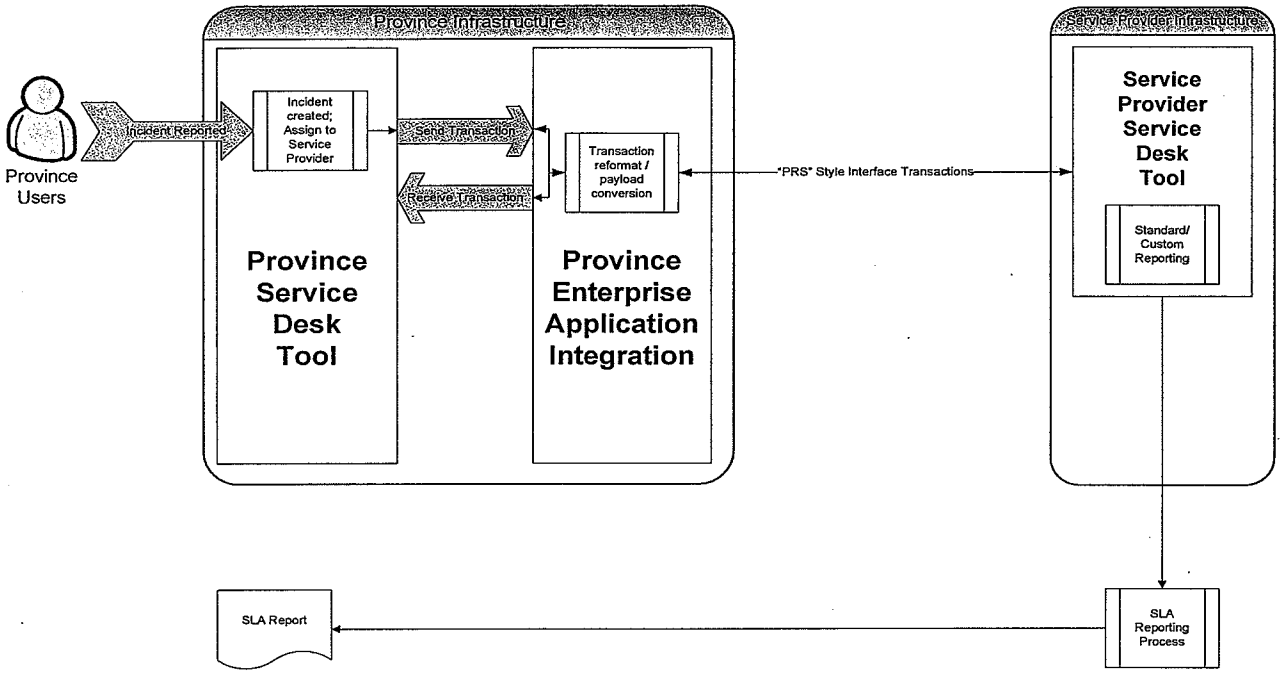
1.11.5 Incident Management Interface

During the first six months following the Hand-Over Date (or such longer period as may be agreed to by the parties through the Change Order Process) the parties will work to develop the interfaces and associated processes and procedures for the exchange of Incident information between the Province Service Desk Tool and the Service Provider Service Desk Tool, all as more particularly described in the Transformation SOW (and referred to in the Transformation SOW as the (the "**Dispatch Interface**" and the "**Non-Dispatch Interface**"). The interfaces that will be developed are generally described in the three scenarios below.

For greater clarification, unless requested otherwise by the Province through the Change Management Process or the Change Order Process, as applicable, the Incidents that will be exchanged through the Service Provider Service Desk Tool and the Province Service Desk Tool will only consist of those Incidents that impact the Services (but all Incidents in the Service Provider Service Desk Tool will be available to the Province for review through the Province's access to the Service Provider Service Desk Tool). The Parties acknowledge that the Province Service Desk Tool and the Service Provider Service Desk Tool will assign different reference numbers to the Incidents.

There are three (3) scenarios in which the Province Service Desk Tool will interface with Service Provider Service Desk Tool, as described below:

(1) *CSC Generated Tickets*: In the first scenario, the Province Client Organizations contact the CSC and an Incident is created in the Province Service Desk Tool. If the Incident is a Major Incident, then the CSC will notify the Service Provider by phone through a single phone number provided by the Service Provider for that purpose. This Incident is forwarded through the Dispatch Interface to the Service Provider Service Desk Tool. The Parties expect that there may be a delay between the creation of an Incident in the Province Service Desk Tool and the creation of a corresponding Incident in the Service Provider Service Desk Tool (the "**Dispatch Interface Delay**"). Refer to the diagram immediately below which depicts this first scenario.



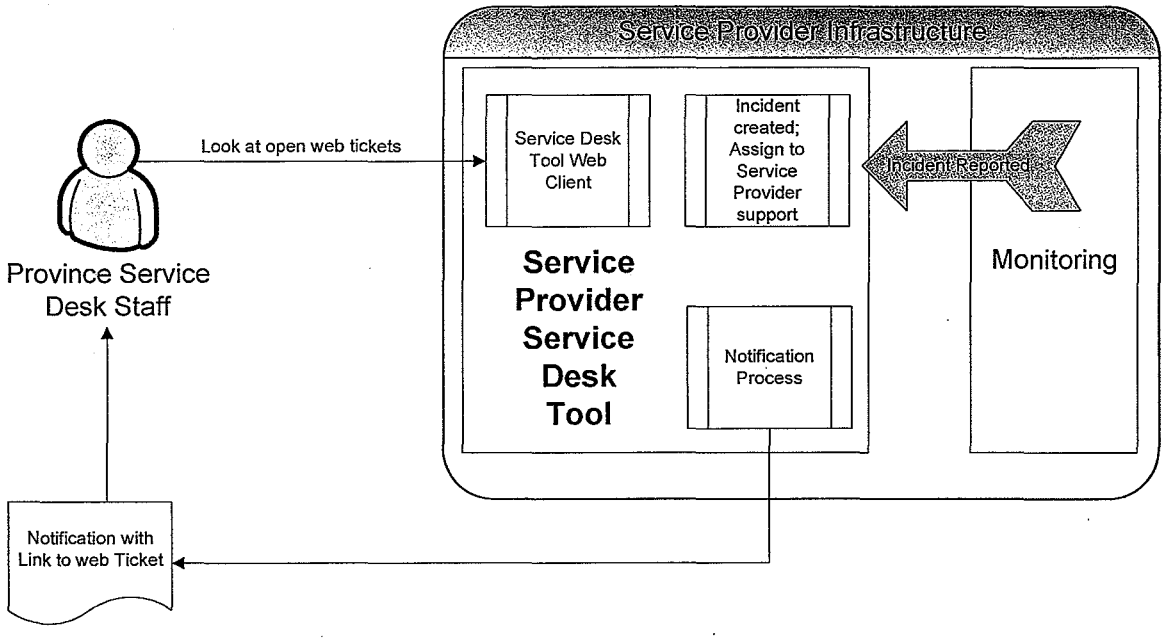
(2) *Bypass Process*: In the second scenario, if the Service Provider becomes aware of a Major Incident that has not been provided to the Service Provider through the Dispatch Interface, then the Service Provider will notify the Province by phone, and if the Incident:

(a) has been created in the Province Service Desk Tool for the Major Incident, but has not been provided to the Service Provider because of the Dispatch Interface Delay, then the Province will advise the Service Provider of the particulars of the Incident by providing the Service Provider with the applicable reference number for the Incident in the Province Service Desk Tool; and

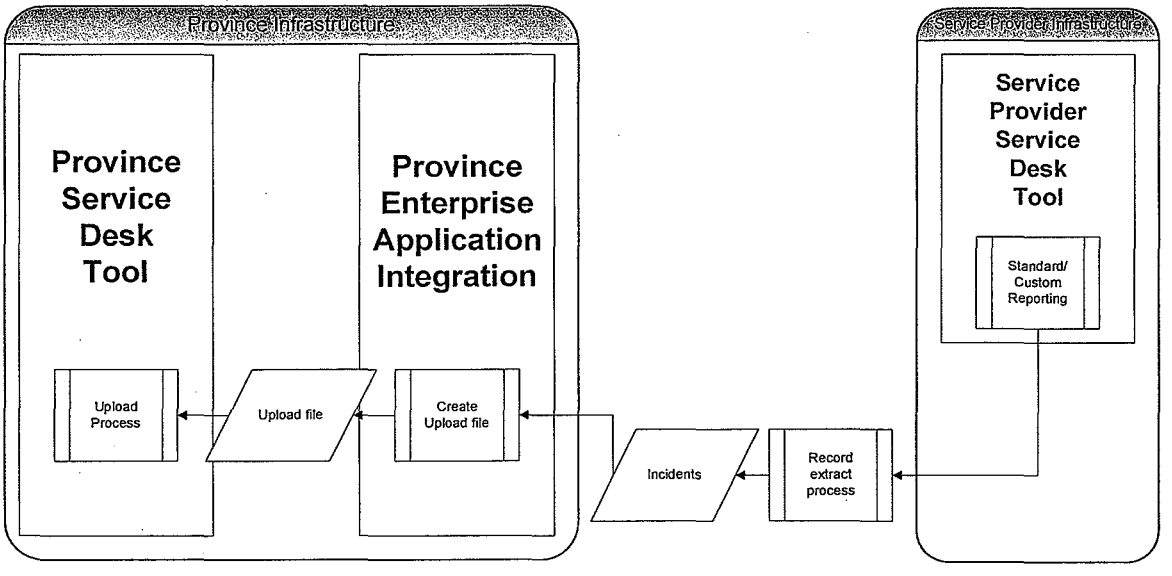
(b) has not been created in the Province Service Desk Tool, then the Service Provider will notify the Province of the Incident by phone and the Service Provider will either provide the particulars of the Incident to the Province by phone or will enter the particulars of the Incident directly into the Province Service Desk Tool, as directed by the Province, and the Province will create the Incident in the Province Service Desk Tool;

(the "**Bypass Process**").

Refer to the diagram immediately below which depicts this second scenario.



(3) *Batch Processing*: In the third scenario, Service Provider will send a daily scheduled batch to Province Service Desk Tool during non-peak hours before 6 a.m. each day (at a specified time agreed to between the Parties, acting reasonably, during the applicable Transformation Project) of all Minor Incidents auto-generated by the Service Provider Service Desk Tool that do not exist in the Province Service Desk Tool and that have not otherwise been sent to the Province Service Desk Tool in the previous batch process (which, for greater clarification, does not include any of the Excluded Minor Incidents, as defined below). Refer to the diagram immediately below which depicts this third scenario.



The Service Provider will determine a process for monitoring and reconciling the Incidents in the Service Provider Service Desk Tool and the Incidents in the Province Service Desk Tool so that the Incidents generated in either tool are synchronized, with the exception of the Incidents

entered into the Service Provider Service Desk Tool that do not impact the Services (the "**Excluded Minor Incidents**"). Following the completion of the Transformation project for the Dispatch Interface and reconciliation process, the Service Provider will provide the Province with satisfactory evidence of such synchronization (initially on a weekly basis, and subsequently on a monthly basis).

The Province Service Desk Tool will be the System of Record for all Incidents that impact the Services. In the event of a discrepancy between data residing in the Service Provider Service Desk Tool and data residing in the Province Service Desk Tool, the data residing in the Province Service Desk Tool shall govern and be used; provided that if Incidents in the Service Provider Service Desk Tool that should be entered into the Province Service Desk Tool are not so entered because the reconciliation process is not properly functioning, then those Incidents will be taken into consideration in calculating the achievement of SLAs and any applicable SLOs.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Incident Management Interface	Province	Service Provider
Verify that the Incidents recorded in the Province System of Record are synchronized with the Incidents recorded in the Service Provider Service Desk Tool (other than the Excluded Minor Incidents). Following the completion of Transformation Projects relating to the Province Service Desk Tool and the Service Provider Service Desk Tool, provide the Province with weekly reports evidencing the synchronization (and reconciliation) of Incidents between the Province Service Desk Tool and the Service Provider Service Desk Tool. Once the Service Provider has established that the synchronization (and reconciliation) process is properly functioning to the reasonable satisfaction of both Parties, then the reports will be provided monthly.		R
Notify the Province by telephone in accordance with the Province's Incident Management Process for all Major Incidents detected by Service Provider before being assigned an Incident reference in the Province's Service Desk Tool, and either notify the Province of the particulars of the Major Incident by phone, or enter the particulars of the Major Incident directly into the Province Service Desk Tool, as directed by the Province.		R
Manually enter all Incidents into Province Service Desk Tool, as may be necessary, in accordance with calls received by the CSC and Major Incidents notified by the Service Provider under the Bypass Process.	R	
Modify, implement and test the Service Provider Service		R

Incident Management Interface	Province	Service Provider
Management Systems when necessary to maintain the use of the Dispatch Interface when changes to applications or infrastructure are initiated by Service Provider.		
Modify, implement and test the Province Service Management Systems when necessary to maintain the use of the Dispatch Desk Interface when changes to applications or infrastructure are initiated by the Province.	R	
When determined to be necessary by the Service Provider, provide to the Province recommendations and suggestions for the evolution of the Province Service Management Systems, for use by the Province as it may determine in its sole discretion.		R
Establish and implement a reconciliation process to synchronize Incident data (other than the Excluded Minor Incidents) between the Province Service Desk Tool and the Service Provider Service Desk Tool and address and resolve discrepancies between them.		R
Notify the Service Provider by telephone in accordance with the Province's Incident Management Process when the Province detects a Major Incident related to the Services.	R	
Provide the Province with one phone number to be used for notifying the Service Provider of Major Incidents.		R
As part of the Transformation Projects relating to the Province Service Desk Tool and the Service Provider Service Desk Tool, implement necessary modifications to the Province Service Management Systems for the purpose of supporting the Dispatch Interface with the Service Provider Service Desk Tool to accommodate the Province System of Record requirements.	R	
As part of the Transformation Projects relating to the Province Service Desk Tool and the Service Provider Service Desk Tool, implement necessary modifications to the Service Provider Service Management Systems for the purpose of supporting the Dispatch Interface with the Province Service Desk Tool to accommodate the Province System of Record requirements.		R

1.11.6 Problem Management

Problem Management is the process applied to minimize the adverse impacts of Incidents for the Province and Client Organizations that are caused by system errors and to prevent recurrence of Incidents related to those errors. Problem Management seeks to find the Root Cause and to initiate and track the actions taken to eliminate the error. A Major Incident will result in the application of the Problem Management Process.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Problem Management	Province	Service Provider
Perform Problem Management for all Problems until such time as the Root Cause is determined by the Service Provider to be unrelated to the Services and the Supported Infrastructure ("**Out of Scope Problems**")		R
Perform Problem Management for Problems that are Out of Scope Problems.	R	
In consultation with the Province, perform the Error Control resolution activities for Problems that are not Out of Scope Problems.		R
Provide input to the Service Provider when the Service Provider consults with the Province regarding Error Control resolution activities for Problems that are not Out of Scope Problems.	R	
Provide information to the Client Organization Contact with respect to the Root Cause of the Problem when it is determined.		R
In consultation with the Province, evaluate and implement Proactive Prevention process or procedure improvements, as determined to be necessary by Service Provider.		R
Provide input to the Service Provider when the Service Provider consults with the Province regarding the evaluations and implementation of Proactive Prevention processes or procedures.	R	
Record, in the Province Service Desk Tool, all Problems identified that are within the scope of the Services by referencing Known Errors to the impacted Problems.		R
Provide to Service Provider guidelines relating to prioritization with respect to the resolution of Problems.	R	
Prioritize resolution of Problems based on impact and urgency using the guidelines provided by the Province (and where there are no such guidelines, then using the criteria set out in the Manual).		R
Perform Root Cause Analysis to investigate the underlying cause of the Problem and identify a temporary Work-around or permanent fix. Once the Root Cause of the Problem is known and a temporary Work-around or permanent fix is identified, classify the Problem as a Known Error.		R
Provide to the CSC information with respect to Known Errors or		R

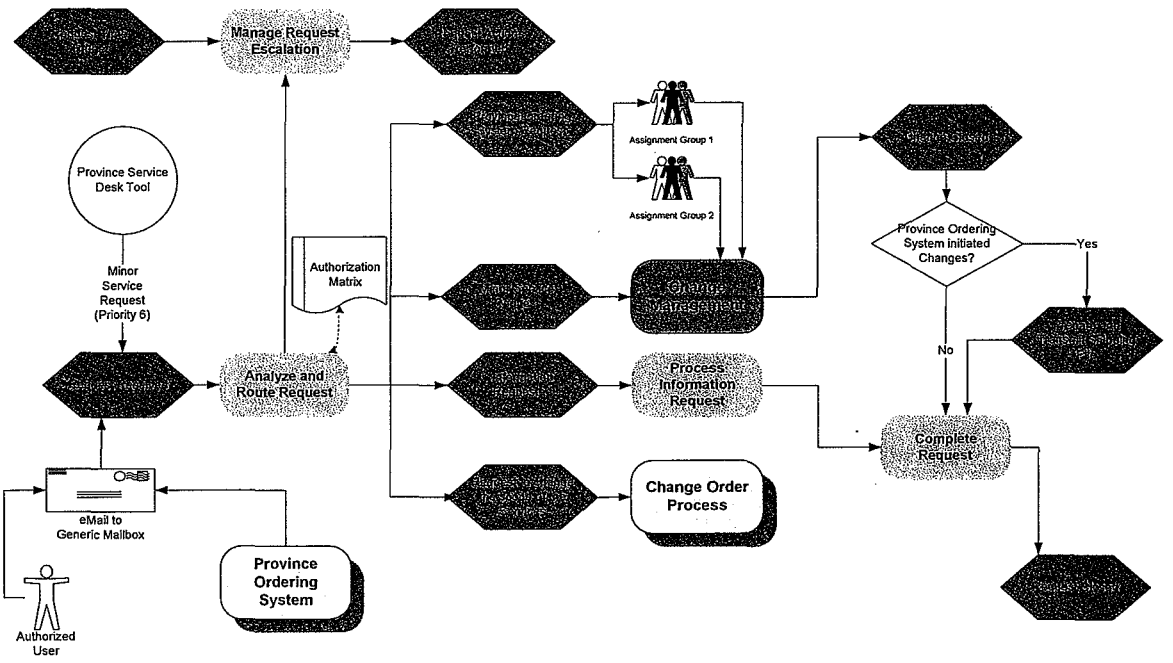
Problem Management	Province	Service Provider
Work-arounds once determined.		
Based upon guidelines provided by the Province or the Manual, as applicable, with respect to the prioritization of Problem resolution, assess the effort and activities necessary to resolve a Known Error and establish a schedule founded on priority, available skills, competing requirements for Personnel to determine the method of resolving the Problem.		R
Submit RFCs to implement the permanent fix for the Known Error and comply with the following in respect of the RFCs: (a) develop, test, and implement the fix and backout procedures; (b) update the Incident Management Application and Change Management Application for permanent fixes within the scope of the Services; (c) close the Problem and Known Error if it exists, once the corrective change has been successfully applied, or the Error is no longer applicable; (d) review the permanent fix to a Problem and consult with the Province to resolve the Problem, for the following: (i) Priority 1 or Priority 2 Incidents; (ii) a series of Priority 3 or Priority 4 Incidents that occur repetitively where it is apparent that they are related; (iii) the underlying cause(s) of the Incident is obvious and related to the Incident; or (iv) the analysis and permanent fix appears to be more cost effective over a short period of time than fixing the repetitive Incident.		R
Maintain information regarding Problem resolutions and temporary fixes, including applicability and effectiveness and communicate to Province the need, if any, for training or retraining of end users.		R
Upon resolution of a Major Problem, determine what was accomplished either correctly or incorrectly and what measures could have been taken to improve the resolution process. Communicate results of the foregoing described process to the Province.		R

Problem Management	Province	Service Provider
Research previous Incidents and Problems in order to identify patterns, volumes and potential Problems and determine if preventative action is required.		R
Initiate Problem Control with respect to Problems as a result of the identification and analysis of patterns and subsequent investigations.		R
Recommend to Province process or procedural improvements as a result of the identification and analysis of patterns. Provide to Province Service Provider feedback regarding testing, procedures, training and documentation.		R
Provide to Service Provider, until resolution of the Problem, updated information for Problems with respect to the WTS services not delivered by the Service Provider that impact or could be reasonably expected to impact the ability of the Service Provider to provide the Services.	R	
Provide to Service Provider within one month of a final Problem resolution, the details of resolution with respect to the WTS services not delivered by the Service Provider that impacted the ability of the Service Provider to provide the Services.	R	

1.12 Request Management

Request Management is the management process for all Requests for service initiated by the Province. This process deals with Requests generated by the Province Ordering System, Minor Service Requests initiated through CSC (Priority 6 tickets), emails to Generic Mailboxes, and phone calls. The purpose of Request Management is to facilitate the tracking and fulfillment of Requests for service received by the Province from Client Organizations. Request Management includes receipt, logging, acceptance, routing by Service Provider, monitoring, fulfillment, documentation and closure of Requests.

As shown in the diagram below, Request Management is the starting point for the coordination, tracking, escalation (both functional and hierarchical) and communication as it relates to Requests.



- Minor Service Requests will be: (1) entered by the Province Level 1 Support in the Province Incident Management Application as Incidents with a priority of 6; (2) sent to the Service Provider through the Generic Mailboxes by an Authorized Requestor; or (3) requested orally by an Authorized Requestor directly to the Service Provider. The Province will assign the Priority 6 Incidents to the appropriate Assignment Group through the CSC. Service Provider will determine the required actions to respond to the Minor Service Request including the submission of an RFC to the Province Change Management Application, if required.

- Province Ordering System Requests are primarily generated though the Province Ordering System. The Province Ordering System Requests are submitted by the Province and Client Organizations, and once they have received the necessary Expense Authority approvals within the Province or Client Organizations, then the Service Provider will be notified by email of the Province Ordering System Request. The Service Provider will obtain the Province Ordering System Request details from the Province Ordering System. Service Provider will determine the required tasks and assign them to the appropriate Service Provider Assignment Group for completion of the Province Ordering System Request. The Service Provider Assignment Group will determine the required actions to complete the Province Ordering System Request including the submission of an RFC to the Province Change Management Application, if required, and the initiation of further Province Ordering System Requests through the Province (EHS), or directly through the Province Ordering System if so determined by the Province and notified to the Service Provider (subject to the Change Management Process or the Change Order Process, as applicable) for services from the Service Delivery Units if required to complete the initial Province Ordering System Request.

- Minor Service Requests to be accommodated through Client Organization's draw down accounts established with the Service Provider may also be received by email (to the

Generic Mailboxes) from Authorized Requestors. Each Service Provider Assignment Group will determine the required actions to respond to the Request including the submission of a RFC to the Province Change Management Application, if required.

- Requests to change the scope of the Services to be provided by the Service Provider under the Agreement (as more particularly described in the Agreement) will be subject to the Change Order Process set out in the Agreement.

1.12.1 Request Management - General Responsibilities

The *Request Management – General Responsibilities* section of this SOW describes the responsibilities of the Parties relating to Request Management services.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Request Management General Responsibilities	Province	Service Provider
Validate the status of the Authorized Requestor based on the information contained in the Authorization Matrix.		R
Record each Minor Service Request received in the Service Provider Service Desk Tool.		R
Establish and communicate to Service Provider a method to redirect Requests that are outside of the scope of the Services.	R	
Redirect to Province those Requests that are outside of the scope of the Services.		R
Determine type of Request, and in the case of Province Ordering System Requests determine the lead times as described in *Appendix N – Request Lead Times*.		R
Assign Request to the appropriate Assignment Group and Service Provider Personnel within the Assignment Group.		R
Monitor the status of completing the Requests and use reasonable efforts to fulfill Province Ordering System Requests within service delivery lead times set out in *Appendix N – Request Lead Times*.		R
Communicate significant expected delays in fulfilling Province Ordering System Requests within service delivery lead times set out in *Appendix N – Request Lead Times* with the applicable Client Organization contacts with a copy to the Province (EHS) (and provide reasons for the delays).		R
Consult with Province as requested from time to time regarding appropriate increases or decreases to be made to the lead times in *Appendix N – Request Lead Times*.		R

Request Management General Responsibilities	Province	Service Provider
Maintain and provide to the Service Provider the protocol for communication with Client Organizations with respect to Request fulfillment.	R	
Comply with protocol established by the Province for communication with Client Organizations with respect to Request fulfillment.		R
Provide responses to Requests for information related to the Services.		R
Communicate, as requested by Client Organization, information regarding progress and fulfillment of Requests within one (1) Business Day.		R
Provide to Service Provider the Province Generic Mailboxes to be used in relation to the Services.	R	
Use Generic Mailboxes for all email communications with Client Organizations with respect to the Services.		R
Transfer Requests to change the scope of the Services to the Change Order Process set out in the Agreement.		R
Submit orders to obtain services from other Service Delivery Units in order to provide the Services through the Province (EHS), or directly through the Province Ordering System if requested to do so in the future by the Province through the Change Management Process or the Change Order Process, as applicable.		R

1.12.2 Province Ordering System Requests

The *Province Ordering System Requests* section of this SOW describes the responsibilities of the Service Provider and the Province for Request Management relating to the use of the Province Ordering System.

Service Provider and the Province will perform the tasks or functions as indicated in the table below.

Province Ordering System Requests	Province	Service Provider
Provide to Province updates, as may be necessary, to the Service Catalogue which relate to the Services.		R
Implement Service Catalogue updates once a month, as may be necessary as determined by the Province, to Province Ordering System which relates to the Services.	R	

Province Ordering System Requests	Province	Service Provider
Provide email notification from Province Ordering System to the Generic Mailboxes to initiate a Request related to the Services.	R	
Monitor Generic Mailbox for email notifications from the Province Ordering System, and obtain the particulars of Province Ordering System requests received from the Province Ordering System.		R
Forward all Province Ordering System Requests with a quote for fees to Expense Authorities for approval and confirm Province Ordering System Requests in accordance with the Server Management Services SOW, as applicable.	R	
For Quoted Orders, facilitate a dialog between Client Organization, WTS and the Service Provider, if necessary, to provide a technical solution, as more particularly described in the Server Management Services SOW.	R	
Provide quotes in response to Quoted Orders received in the Province Ordering System with respect to the Services for which a quote is required.		R
Apply financial approval for orders in the Province Ordering System, as determined in the Province's discretion.	R	
Coordinate Province Ordering System Requests through Service Provider Assignment Groups, and notify other Service Delivery Units of the Province Ordering System Request order number in the Province Ordering System where the initial Province Ordering System Request also contains a request for services from other Service Delivery Units.		R
Fulfill orders received from the Province Ordering System with Expense Authority approval.		R
Create Shipping Files and initiate updates to Province Ordering System as Requests are fulfilled by the Assignment Groups.		R
Resolve Shipping Errors and re-ship as may be required, within three (3) Business Days of receiving a Shipping Error.		R
Reject those orders within the Province Ordering System that are submitted with errors or that Service Provider cannot fulfill. Provide explanation for rejection to the Province.		R
Make available to Service Provider information (documented where possible) with respect to the Province Ordering System Shipping Errors.	R	
Where the Service Provider receives an email notice from the		R

Province Ordering System Requests	Province	Service Provider
Province Ordering System of a Province Ordering System Request that involves other Service Delivery Units, the Service Provider will notify the other Service Delivery Units of the request by email.		
Where the Service Provider receives an email notice from the Province Ordering System of a Quoted Order that involves other Service Delivery Units, the Service Provider will notify the other Service Delivery Units of the Quoted order, and Service Provider will not accept the Quoted Order until the other applicable Service Delivery Units have provided the required quotes for the Quoted Order.		R
Provide and maintain the report format and method for the Service Provider to post monthly reports (for Province billing purposes) for shared service storage consumption and SFP home drives for Client Organizations who self-manage their SFP home drives.	R	
Produce and provide monthly reports (for Province billing purposes) for shared services storage consumption by Client Organization that is not automatically generated by the Province Ordering System.		R
Produce and provide monthly reports (for Province billing purposes) for SFP home drives for Client Organizations (who self-manage their SFP home drives) that are not automatically generated by the Province Ordering System.		R

1.13 After Hours Service Desk (Optional Service)

The After Hours Service Desk services are an optional service that will only be included as part of the Services if the Province determines, in its discretion, to procure the After Hours Service Desk from the Service Provider pursuant to the Change Order Process. The general responsibilities of the Parties described in Sections 1.7 and 1.11.1 (and to the extent applicable 1.12.1) above will apply to the After Hours Service Desk services. For greater clarification, the Province may purchase the same or similar services to the After Hours Service Desk services from another vendor (in lieu of the Service Provider) or may provide such services itself on an in-house basis.

The After Hours Service Desk services consists of logging calls and dispatching to the appropriate Assignment Group, where appropriate, Incidents received from the Province for all WTS services (including the Services provided by the Service Provider), but excluding Workstation Services.

The CSC After Hours Service Desk hours of operation in Pacific Time are as follows (the "**After Hours**"):

- Monday 7:00 PM to Tuesday 7:00 AM
- Tuesday 7:00 PM to Wednesday 7:00 AM
- Wednesday 7:00 PM to Thursday 7:00 AM
- Thursday 7:00 PM to Friday 7:00 AM
- Friday 7:00 PM to Monday 7:00 AM
- Statutory Holidays
- 1 hour of coverage per calendar month to provide coverage during scheduled CSC Monthly Staff Meetings and during emergency test procedures (such as fire drills)

The table below describes the responsibilities of the Province and the Service Provider relating to the After Hours Service Desk services.

After Hours Service Desk	Province	Service Provider
Provide to Province a single telephone number for the Service Provider Voice Response Unit for purposes of providing the After Hours Service Desk services.		R
Make the Incident Management Application for automated tickets generated during After Hours available to the Service Provider.	R	
Monitor the Incident Management Application for automated tickets generated during the After Hours and re-assign tickets to the appropriate Assignment Group.		R
Maintain and make available to Service Provider relevant CSC Online Procedures for the After Hours Service Desk services.	R	
Provide an initial assessment: (a) classify reported Incidents according to *Appendix L - Incident Prioritization Matrix* and create a ticket for the Incident in the Incident Management Application; (b) receive and deal with inquiries or complaints and log all such calls and responses in the Incident Management Application; (c) respond to questions regarding open Incidents and log all such calls and responses in the Incident Management Application; (d) process Minor Service Requests and questions directed to the Service Provider using the Request Management Process; (e) assign Incidents to appropriate Assignment Groups based upon written troubleshooting procedures in the CSC Online Procedures made available to the Service Provider;		R

After Hours Service Desk	Province	Service Provider
(f) advise the After Hours user of the Workstation Services helpdesk number (provided by the Province) for and applications support, as appropriate; and (g) assign Incidents to the appropriate Level 2 or 3 Support.		
Perform Call-Outs for all Major Incidents received by the After Hours Service Desk upon receipt.		R
Route Single Point of Contact Option 3 After Hours calls to After Hours Service Desk.	R	
Escalate Incidents in accordance with the CSC Incident Management and Escalation Procedure set forth in the CSC Online Procedures made available to the Service Provider (during the transition of the After Hours Service Desk to the Service Provider, if such services are procured by the Province).		R
Make available to the Client Organization Contact the status of the Incident, as requested by the Client Organization Contact.		R
Monitor Incidents on a daily basis, and review any related issues or problems with Service Provider as they arise, relating to quality and accuracy of information logged by the After Hours Service Desk regarding the Incident.	R	
Participate in any reviews requested by the Province as a result of its daily monitoring of Incidents for quality and accuracy of information logged by the After Hours Service Desk regarding the Incident.		R
Arrange and chair weekly conference calls with Service Provider to review Incidents and After Hours Service Desk service issues.	R	
Participate in the weekly conference calls arranged by the Province to review Incidents and After Hours Service Desk service issues.		R
Track the Incident to resolution (which resolution may occur at the Level 2 or Level 3 Support) and close Incidents in the Province's Incident Management Application for Incidents that have been resolved.	R	
Communicate with Client Organizations with respect to Major Incidents that occur or continue After Hours, in accordance with the communication procedures set out in the Manual (and developed in consultation with the Province as described above under Section 1.7), which communications may occur during the After Hours or at such other times as determined by the Province and notified to the Service Provider.	R	

Appendix A – Definitions – Service Management Services SOW

Definable Term	Definition
"Access Rights Contracts"	Has the meaning given to it in the Master Transfer Agreement.
"After Hours"	Outside of the CSC Hours of Operation.
"After Hours Service Desk"	Service Desk that supports all WTS services (including the Services provided by the Service Provider), but excluding Workstation Services, outside of the CSC Hours of Operation.
"Asset Management Services"	The management of the Hardware and Software Assets, throughout their lifecycles, used to deliver the Services, as more particularly described in this SOW.
"Assignment Group"	The Level 2 Support and Level 3 Support personnel dedicated to a specific technical function.
"Authorization Matrix"	A list of Province Staff and their alternate(s) who can authorize and approve Requests with respect to the Services.
"Authorized Requestor"	Individual authorized to submit Requests to the Service Provider.
"Booked Order"	An order in the Province Ordering System that has received financial approval by the applicable Expense Authority.
"Business Day"	Has the meaning given to it in the Agreement.
"Call-Outs"	The act of contacting the appropriate individual(s) to engage them in work.
"CAS Install Base"	Repository used for WTS financial recovery and billing by the Corporate Accounting Services organization within Shared Services B.C.
"Change"	Ordinary Course Changes (as defined in the Agreement), Major Changes, Significant Changes, Minor Changes, Emergency Changes or Change Orders to modify the Supported Infrastructure or change the Services received by a Client Organization (but excludes amendments or modifications top the Agreement).
"Change Freeze Period"	A Request by Client Organization or other Service Delivery Unit to place in abeyance any planned changes to specific underlying infrastructure during a specified period, and in all cases will

Definable Term	Definition
	exclude emergency and security related changes.
"Change Management"	The management of Changes in the manner provided for under this SOW.
"Change Management Application"	The Province's application used to manage Changes which forms part of the Province Service Desk Tool.
"Change Management Process"	The Province's process for managing the planning, implementation and post-implementation reviews of all Changes and the handling of any resulting Incidents with minimum disruption.
"Change Management Coordinator"	A Province Staff member who is indicated in the Authorization Matrix as the "Change Management Coordinator".
"Change Order Process"	Has the meaning given to it in the Agreement.
"Change Window"	Period of time allocated for implementing Changes which may include planned outages as applicable during which time Changes may be implemented, as set forth in *Appendix J – Province Change Windows*.
"Client Ministry"	Ministry of the Province of British Columbia that receives Services.
"Client Organization"	A party that receives the Services consisting of a Client Ministry, WTS or a Broader Public Sector organization.
"Contact"	Client Organization Staff member who contacts and liaises with the CSC or Service Provider regarding an Incident, Change or Problem.
"CSC"	Province Level 1 Support entry point for all of WTS services (excluding Workstation Services).
"CSC Hours of Operation"	Normal business hours for the Province CSC consisting of: Monday to Friday 7:00 AM to 7:00 PM Pacific Time, excluding Statutory Holidays.
"CSC Monthly Staff Meeting"	The meeting of the Staff of the CSC that is held for a period of one (1) hour each calendar month.
"CSC Procedures"	The Province's Incident Management documentation for all processes and procedures used for managing and updating Incidents in the Province Service Desk Tool, as may be updated and amended from time to time by the Province through the Change Management Process or the Change Order Process, as applicable.

Definable Term	Definition
"CSC Online Procedures"	The Province's online documentation for Incident processes and procedures, Incident Management SLAs, call handling, call-out procedures and WTS contact information, as may be updated by the Province from time to time.
"Emergency Change"	A Change that must be implemented to address an existing failure or security threat, or prevent a likely failure or security threat, before the next scheduled Change Window.
"Error Control"	Process that involves the identification, recording, and assessment of Known Errors. Once the solution to a Known Error is implemented, the process records, closes and monitors the progress of a resolution.
"Escalation Procedure"	The process of progression by which increasingly higher levels of authority are engaged to resolve a matter.
"Expense Authority"	An officer of the Province with delegated authority to approve expenditures or payment requisitions within the available appropriation.
"Fire Season"	Period of time when there is forest fire activity in the Province as designated by the Forest Protection Branch of the Province of British Columbia.
"Forward Schedule of Changes"	Collection of reports posted on the WTS website for communications regarding changes to be implemented in the next 7 or 14 calendar days.
"Generic Mailbox"	These are email IDs set up for Assignment Groups to receive and send communication from/to Client Organizations (sometimes referred to as a group mailboxes).
"Hardware Asset"	Physical equipment having a purchase value (including any applicable taxes) of greater than one thousand dollars ($1,000) and which is depreciable and is used to provide the Services.
"Hardware Asset Data Elements"	Hardware attributes that are collected and managed by the Service Provider, as more particularly described in *Appendix F – Hardware Asset Data Elements*.
"Hardware Asset Management"	The management of physical equipment used to provide the Services, as more particularly described in this SOW.
"Incident"	Any event which is not part of the standard operation of a service (including the Services provided by the Service Provider) and

Definable Term	Definition
	which causes, or may cause, an interruption or a reduction of the quality of that service.
"Incident Management"	A collection of activities and processes to restore normal operations as quickly as possible with the least possible impact on either the business or the user, in a commercially reasonable manner.
"Incident Management Application"	The Province's application used to manage Incidents which forms part of the Province Service Desk Tool.
"ITIL"	A set of concepts and policies for managing information technology infrastructure, development and operations.
"Known Error"	A fault identified by the successful diagnosis of a Problem and for which a temporary Work-around or a permanent solution has been identified.
"Lead Times"	The minimum notification time required prior to the approval and implementation of a Change, a Request or a TIB, as applicable.
"Level 1 Support"	First point of contact for support for Client Organizations.
"Level 2 Support"	Entry level technical Service Provider Personnel assigned to help Client Organizations resolve Incidents or Problems.
"Level 3 Support"	Senior level technical Service Provider Personnel assigned to help Client Organizations resolve Incidents or Problems.
"LOB Applications"	Any software developed or purchased to support WTS or Client Organization businesses.
"Major Change"	A change that has the potential to impact the majority of Province Users that has a designated severity of High or Medium, and includes any SFP Changes that may impact Client Organizations.
"Major Incident"	Any Incident that meets the criteria for Priority 1 or Priority 2.
"Major Problem"	Any Problem that is suspected of causing Major Incidents.
"Manual"	Has the meaning given to it in the Agreement.
"Ministry of Labour and Citizens' Services"	The "Ministry of Labour and Citizens' Services" within the Province, as such Ministry may be renamed or organized from time to time, and includes any successor Province entity to the Ministry.

Definable Term	Definition
"Minor Change"	A change that does not impact the Client Organizations and has a designated severity of Low or Informational.
"Minor Incident"	Any Incident that does not meet the criteria for Priority 1 or Priority 2.
"Minor Service Request"	Any Request related to the Services that does not have a financial implication and is not orderable through the Province Ordering System and is received by way of: (a) Priority 6 Incidents from the Province Incident Management Application; (b) emails to Generic Mailboxes; or (c) as otherwise agreed to by the Parties.
"Operating System"	An interface between hardware and applications responsible for the management and coordination of activities and the sharing of the limited resources of the computer.
"Option 3"	Phone tree selection when calling Shared Services B.C. Single Point of Contact that connects the caller to the CSC.
"Owned"	Asset that has been purchased outright, is leased or is licensed by a Party.
"Pacific Time"	The time zone applicable to the Province of British Columbia. The Pacific Time Zone observes standard time by subtracting eight hours from Coordinated Universal Time (UTC-8). During daylight saving time, its time offset is UTC-7.
"Personnel"	Has the meaning given to it in the Agreement.
"Priority 1", **"Priority 2",** **"Priority 3",** **"Priority 4",** **"Priority 5",** **"Priority 6"**	Each has the meaning given to it in *Appendix L - Incident Prioritization Matrix*, as applicable for Incidents, Problems and Minor Service Requests.
"Proactive Prevention"	Activities undertaken to prevent the future occurrence of a known Problem.
"Problem"	A state, identified from Incidents, that indicates an error in the

Defined Term	Definition
	Supported Infrastructure.
"Problem Control"	Process that involves the identification, recording, classification, investigation and diagnosis of Problems focuses on transforming Problems into Known Errors.
"Problem Management"	Process to minimize the adverse impacts of Incidents and Problems that are caused by errors, to prevent recurrence of Incidents and Problems related to these errors, and to determine the Root Cause of the error and initiate and track action to remove the error.
"Problem Management Application"	The Province's application used to manage Problems which forms part of the Province Service Desk Tool.
"Province (EHS)"	Has the meaning given to it in the Server Management Services SOW.
"Province Maintenance Agreements"	Has the meaning given to it in the Master Transfer Agreement.
"Province Ordering System"	Application and infrastructure, interfaces and workflows that allow Client Organizations to purchase, modify or cancel WTS services (initially known as "iStore").
Province Ordering System Requests	An order made through the Province Ordering System for Services that can be provided by the Service Provider.
"Province Partners"	Any private sector entity that provides services other than the Services to the Province.
"Province Service Desk Tool"	Application and infrastructure owned by the Province to coordinate all the service management functions consisting of Incident, Problem, Change, Request and Asset Management.
"Province User(s)"	Consists of personnel in Client Organizations and WTS who are the end-users of any part of the Supported Infrastructure.
"Purchasable Item"	A service that can be purchased through the Province Ordering System.
"Quoted Order"	A Purchasable Item in Province Order System that does not have a price associated with it, for which a price quote will be provided.
"Request"	A Minor Service Request or a Province Ordering System Requests, as applicable.

Definable Term	Definition
"Request Management"	A collection of activities to process and control all Requests for service initiated by the Province and to facilitate the tracking and fulfillment of Requests.
"RFC"	A written request through the Province's Change Management System for a Change to be made that includes details of the proposed Change.
"Root Cause"	A specific reason or group of reasons that can be logically identified, as causing an error, Incident or Problem, as applicable, which, once remedied, should prevent the recurrences of the error, Incident or Problem.
"Root Cause Analysis"	Methodology for identifying and correcting the Root Cause of an error, Incident or Problem (as opposed to troubleshooting and problem solving that seeks immediate solutions to resolve the user visible symptoms).
"Service Bulletin"	A short high level summary of a TIB, which, for greater clarification does not include the technical details in the TIB.
"Services"	Has the meaning given to it in the Agreement.
"Service Delivery Unit"	A division within WTS that provides services.
"Service Desk Tool"	Service Management application and associated infrastructure used to support service delivery to the Province.
"Service Management Systems"	Refers to the infrastructure, associated applications and methodologies consisting of the Service Desk Tool, messaging applications, network and computer equipment, and application integration brokers.
"Service Provider Service Desk Tool"	Application and infrastructure owned by the Service Provider to coordinate all the service management functions consisting of Incident, Problem, Change, Request and Asset Management (initially known as "Digital Workflow").
"SFP"	Shared File and print services, as more particularly described in the Shared File and Print SOW.
"Shared Services B.C."	Division within the Ministry of Labour and Citizens' Services that provides shared support services for public sector organizations to better serve the people and businesses of British Columbia.

Definable Term	Definition
"Shipping File"	A collection of service record updates that indicate fulfilment of services and that are sent to Province Ordering System so that the services may be billed to the applicable Client Organization.
"Shipping Error"	Notification that a service record update was rejected by the Province Ordering System due to an error.
"Significant Change"	A change that has the potential to impact a group of users in one or two Client Organizations.
"Significant Event Review"	Process to review the circumstances, actions, adherence to process of a Change, series of Changes, an Incident, multiple Incidents (related to the same Client Organization or service), or a project that includes multiple Change, which process focuses on what happened, where improvements can be realized and recommended actions to address failures or improve service, as more particularly described in *Appendix M - Significant Event Review*.
"Single Point of Contact"	Single point of contact service desk for WTS (initially 250-387-7000).
"Software Asset"	Software having a purchase of value (including any applicable taxes) of greater than one hundred dollars ($100) and which is depreciable and is used to provide the Services.
"Software Asset Management"	The management of Software Assets used to provide the Services, as more particularly described in this SOW.
"Standard RFCs"	A repeatable activity with a known outcome, where the outcome has been communicated to the Client Organization, the risk of achieving an unanticipated outcome is minimal, and the Province has approved of the activity as being classified as a "Standard RFC".
"Statutory Holiday"	Any statutory holiday applicable in the Province of British Columbia.
"Staff"	Employees and independent contractors of the Province and Client Organizations (but excluding the Service Provider and any of the Service Provider's Personnel).
"Supported Infrastructure"	Has the meaning given to it in the Security SOW.
"System of Record"	The Province Service Desk Tool containing the master records used to resolve discrepancies and inconsistencies between the Province

Definable Term	Definition
	Service Desk Tool and the Service Provider Service Desk Tool with respect to Incidents, Problems and Change Management.
"Technical Peer Review"	Senior technical support personnel who review Changes for technical conflicts and impact.
"TIB"	Province technical information bulletin to notify Client Organizations of Major Changes that may or may not require action on the part of Client Organization.
"Use Rights"	Has the meaning given to it in the Master Transfer Agreement.
"Voice Response Unit"	The interaction between a human (typically a caller) and a computer that is programmed to respond to the human's requests, also referred to as interactive voice response (commonly abbreviated to IVR), which is a computer phone application that accepts touch-phone keypad selection input from the caller and provides appropriate information in the form of voice answers or a connection to a "live" operator.
"Work-around"	A method of avoiding an Incident or Problem, by employing a temporary fix or technique.
"Workstation Services"	A service responsible for desktop computers, laptop computers, some Desktop Terminal Services ("DTS"), and local printer and local network print devices.
"WTS"	Has the meaning given to it in the Agreement.
"WTS service"	All services delivered to Client Organizations by the WTS Staff, Province Partners or the Service Provider.

Appendix B – Service Management Reporting

The following table lists the standard reports that will be provided to the Province nine (9) months after the Hand-Over Date. These reports are categorized in accordance with the sections within the Service Management SOW, each of which describes a component of the Service Management Services.

MONTHLY:

Monthly reports will be generated and delivered by the Service Provider to the Province within ten (10) Business Days of the last calendar day of the month.

WEEKLY:

Weekly reports will be generated and delivered by the Service Provider to the Province within one (1) Business Day of each Friday.

Report Reference	Subject Matter Category	Title of Report	Description of Report Contents	Report Frequency
1	Asset Management	Province Owned Software Asset	Organized by Client Organization with Data Elements agreed by both parties for the purpose of assisting CSC in triaging tickets	Monthly
2	Asset Management	Service Provider Owned Software Asset	Organized by Client Organization with Data Elements agreed by both parties for the purpose of assisting CSC in triaging tickets	Monthly
3	Asset Management	Province Owned Hardware Asset	Organized by Client Organization with Data Elements agreed by both parties	Monthly
4	Asset Management	Service Provider Owned Hardware Asset	Organized by Client Organization with Data Elements agreed by both parties	Monthly
5	Asset Management	Province Owned Assets Scheduled for Retirement	List of Province Owned assets with expiration/retirement date between 3 to 6 months, organized by Client Organization with Data Elements agreed by both parties	Monthly
6	Asset Management	Service Provider Owned Assets Scheduled for Retirement	List of Service Provider Owned assets with expiration/retirement date between 3 to 6 months, organized by Client Organization with Data Elements agreed by both parties	Monthly

Report Reference	Subject Matter Category	Title of Report	Description of Report Contents	Report Frequency
7	Change Management	Change Management Summary	# of Changes rolled back, reasons; # of Changes unexecuted, reasons; # of Changes implemented without full approval, reasons; # of Changes caused incidents, including incident ticket & reasons; # of Changes incomplete, reasons; # of Changes successful but not as documented, reasons.	Monthly
8	Incident Management	Incident Reconciliation Summary	Report back on Server Provider Service Desk Tool Incidents vs. Province Service Desk Tool Incidents based on all Priorities. How many Server Provider Service Desk Tool Incidents were recorded and how many Province Service Desk Tool Incidents were recorded for trend analysis. Number of Incidents based on all priorities including Requests (P6) and Problems (P5) opened and closed.	S. 15
9	Incident Management	Problem Management & Root Cause Summary	List of Problem (P5) opened and closed and associated RCA text.	S. 15
10	Request Management	Province Ordering System Request Summary	Province Ordering System Request Summary setting forth the following for those Province Ordering System Requests for which there is an SLA or SLO: # orders received by assignment group # orders shipped within lead time, # orders shipped exceed lead time, # orders waiting for fulfilment	Monthly

Report Reference	Subject Matter Category	Title of Report	Description of Report Contents	Report Frequency
11	Request Management	Minor Service Request Summary	List of Province Service Desk Tool P6 tickets order by Assignment Group, # open, # closed and the service descriptions	Monthly
12	After Hours Service Desk (if service is provided by the Service Provider)	Operations Report	Total calls recorded: Compare how many calls were received via the phone queue, how many of these were recorded as Incidents in the Province Service Desk Tool, how many were recorded "ITIMS CALLS" in the Province Service Desk Tool to determine first call resolution. All phone calls that are received via phone queue should either have a corresponding call or Incident number, one for one. Incident quality based on incident requirements that are documented. Average Speed of answer, Average talk time per call, Average wait time in the queue, Total calls offered, Abandoned calls	Weekly then move to monthly

Appendix C – Systems

Intentionally Left Blank

Appendix D – Support Customer Locations

Intentionally Left Blank

Appendix E – Service Provider Service Locations

Intentionally Left Blank

Appendix F – Hardware Asset Data Elements

Service Provider will manage the Data Elements listed below with respect to Hardware Assets used to provide the Services.

Data Element	Definition	Source
Address 1	Street address (Physical).	Base Inventory Extract
Address 2	Additional address detail (Physical).	Base Inventory Extract
Municipality	Municipality where asset primarily resides.	Base Inventory Extract
Province	Province where asset primarily resides.	Base Inventory Extract
Postal Code	Postal code where asset primarily resides.	Base Inventory Extract
Country	Country where asset primarily resides.	Base Inventory Extract
Location Code	Building location code ("BLC") of location or sublocation code (for example, grid tile).	Base Inventory Extract
Manufacturer	Manufacturer of the asset.	Base Inventory Extract
Model Name	Model name typically located on front of asset.	Base Inventory Extract
Nature	Model type (for example, desktop PC, notebook, and so on).	Base Inventory Extract
Serial Number	Identifying number from OEM (desktop, laptop, and server).	Base Inventory Extract
Asset tag number (Also referred to as Asset tag)	Province asset tag numbers - 2 numbers from different sources: Asset management tool (e.g., Remedy) Province Ordering System/CAS Install Base asset tag, if one exists.	Base Inventory Extract
Service Provider Asset Tag	J-Tag for items under fixed asset capitalization limits or that are Province owned.	Scan or Manual Entry
Status	Active, retired, idle.	Drop down during inventory
Asset Owner (also referred to as Asset Managed)	Asset owned by Province or Service Provider to deliver the Services to Client Organization will be identified by an organization code ("org code").	Province provided
UNSPSC	Model classification.	Link to model table
Cost Centre	Service Provider financial center asset is billed to or Province cost center.	Province provided
External PO #	Service Provider created PO number for Service Provider owned assets or the External PO number created for Province owned assets that is used to obtain the hardware from the supplier.	Province provided
System Name/Server Name	Internal name given to the asset.	Manual entry

Data Element	Definition	Source
Client Organization	See Appendix A definition.	Service Provider Service Desk Tool
Fully Qualified Domain Name	Server and internet domain name for a particular System (such as *[server name].[Client Organization Code]*.gov.bc.ca).	Service Provider Service Desk Tool
IP address	Internet protocol number assigned to a device in the network.	Service Provider Service Desk Tool
MAC Address	Media access control number assigned to a hardware component of a System.	Service Provider Service Desk Tool

Appendix G – Software Asset Data Elements

Service Provider will manage Data Elements listed below with respect to those Software Assets used to provide the Services.

Data Element	Definition	Source Responsibility	Required for Software Asset Tracking
Province	Four character code to define management responsibility for the software license.	Service Provider	Software Asset Tracking
Assignment	Disposition of this license: in use, in stock, retired, awaiting receipt, returned for maintenance, returned to supplier.	Province	Software Asset Tracking
Quantity	Quantity of licenses.	Province	Software Asset Tracking
In-service date	The date that a repository record becomes active	Service Provider	Software Asset Tracking
Support group	The team that actually supports the software license, for Province supported tracked by Service Provider, the value is ACCOUNT, and otherwise it will be a Service Provider Asset Support team.	Service Provider and Province	Software Asset Tracking
Location	The Service Provider business location code that represents the place where the asset is installed.	Province	Software Asset Tracking
Model	The software license, including the technical reference and manufacturer.	Province	Software Asset Tracking
Cost Center	Code that represents Service Provider financial mapping structure.	Service Provider	Software Asset Tracking
Component of	Parent of this software license, either a hardware device or another license.	Province	Software Asset Tracking
Asset Managed (also referred to as Asset Owner)	Asset owned by Province or Service Provider to deliver the Services to Client Organization will be identified by an organization code ("org code").	Province	Software Asset Tracking
Point of Delivery	Code for the service, information, or data center facility where license resides.	Service Provider	Software Asset Tracking
Serial #	License serial number, can be vendor supplied and/or a Province/Service Provider developed number to identify the asset.	Province	Software Asset Tracking

Data Element	Definition	Source Responsibility	Required for Software Asset Tracking
Asset tag (Also referred to as Asset tag number)	Province asset tag numbers - 2 numbers from different sources: Asset management tool (e.g., Remedy) Province Ordering System/CAS Install Base asset tag, if one exists.	Service Provider	Software Asset Tracking
Status	Disposition of the asset/batch record for the asset.	Province	Software Asset Tracking
Installation Date	Relates to the date the software product was installed by Service Provider.	Service Provider	Software Asset Tracking
Remarks	Service Provider free form comments relating to asset.	Service Provider	Software Asset Tracking
Supplier	Vendor or manufacturer of Software Asset.	Service Provider /Province	Software Asset Tracking
Acquisition Method	Purchase, rental, lease	Service Provider /Province	Software Asset Tracking
Purchase Order (PO) Number	The purchase order number that is generated by the internal Service Provider procurement system on the order.	Service Provider	Software Asset Tracking
External Purchase Order Number	The purchase order number that was used to obtain the software license from the supplier.	Province	Software Asset Tracking
Operating System	Operating system that related to this Software Asset.	Province	Software Asset Tracking
Single/Multiple	Identifies the user type for the Software Asset.	Province	Software Asset Tracking
Province License Type	Describes how the vendor sells or licenses the Software Asset whether by CPU, site, enterprise, or server.	Province	Software Asset Tracking
License Size	Free form vendor supplied tiering structure for asset.	Province	Software Asset Tracking
License Owner	Organization code for Province that owns asset.	Province	Software Asset Tracking
Expiration Date	Renewal date for the software license.	Province	Software Asset Tracking
Compute Platform	Operating platform where the software is allowed to execute.	Province	Software Asset Tracking
Password Expiration Date	Renewal date for software password.	Province	Software Asset Tracking

Data Element	Definition	Source Responsibility	Required for Software Asset Tracking
Rights	Software user rights per the vendor of the asset.	Province	Software Asset Tracking
Password Type	The type of security solution the supplier has placed on the software license usability (zap, password, key, and so on).	Province	Software Asset Tracking
Conditions (both warranty and maintenance)	Conditions for the maintenance and warranty contracts consisting of exclusions, terms, coverage, and range.	Province	Software Asset Tracking
Maintenance start/end dates	Maintenance contract start and end dates.	Province	Software Asset Tracking
warranty expiration	Expiration date for warranty contract.	Province	Software Asset Tracking
Client Organization	See Appendix A definition.	Service Provider Service Desk Tool	Software Asset Tracking
Requestor Name	Name of applicable Service Provider Personnel who requests the Software on behalf of the Client Organization.	Service Provider Service Desk Tool	Software Asset Tracking
Description / Comments	Description of the Software and purpose for the Software.	Manual	Clarification of purpose of Software

Appendix H - Change Categories and Lead Times

The following Change category table describes the Change categories and the associated lead times, subject to the TIB Guidelines set forth in *Appendix P - TIB Guidelines*, which may require longer lead times for specific RFCs. "Minimum Review Lead Time" in the table below means the minimum notification time from the later of (i) receipt of the RFC by the Province in the Province's Change Management Application, and (ii) receipt by the applicable individuals whose approval is required as per the Authorization Matrix, prior to the planned start for the implementation of a Change (the "**RFC Receipt Date**"). "Minimum Approval Lead Time" in the table below means the minimum period of time prior to the planned start for the implementation of a Change by which the Service Provider requires approval of the Change from the applicable individuals whose approval is required as per the Authorization Matrix.

In calculating the lead times, the date that the RFC Receipt Date occurs is included where the RFC Receipt Date occurs prior to 12:00 p.m. PST (and if the RFC Receipt Date occurs after 12:00 p.m. PST, then the date that the RFC Receipt Date occurs is excluded), and in each case the planned start date for the implementation of a Change is excluded.

Change Categories and Lead Times Table

Change Category Description	Minimum Review Lead Time	Minimum Approval Lead Time
Major Change	Ten (10) Business Days	Five (5) Business Days
Significant Change	Five (5) Business Days	Two (2) Business Days
Minor Change	One (1) Business Days	One (1) Business Day
Emergency Change	In the case of addressing a failure or security threat, no lead time is required. In the case of preventing a failure or security threat, Service Provider will give notice to the Province by 13:00 PST to the extent possible on the planned implementation date for the Change.	In the case of addressing a failure or security threat, approvals may be granted after the Change is implemented. In the case of preventing a failure or security threat, approvals are granted as soon as possible as per the Authorization Matrix and the Province's Change Management Coordinator.

Appendix I - Assessment of Severity

The assessment of the severity of a Change is based upon the Backout Effort, Risk, Impact and Exposure of the Change (each as defined in the Change Management Application and reproduced below) as determined by readily available information from the RFC. The Technical Peer Review will review the severity elements set forth in the table below and may change the ranking in any one or more of the elements, resulting in a different severity being assigned to a Change.

The severity of a Change has one of four possible values: **LOW ("L")**, **MEDIUM ("M")**, **HIGH ("H")** and **INFORMATIONAL ("I")**. The severity is determined by an aggregate assessment of Backout Effort, Risk. Impact and Exposure as illustrated in the following table.

Table 1. Determination of Severity based on Backout Effort, Risk, Impact and Exposure.

CHANGE MANAGEMENT SEVERITY MATRIX				
Backout Effort	**Risk**	**Impact**	**Exposure**	**Severity**
L	L	L	L	I
L	L	L	M	I
L	L	L	H	M
L	L	M	L	L
L	L	M	M	M
L	L	M	H	H
L	L	H	L	M
L	L	H	M	M
L	L	H	H	H
L	M	L	L	L
L	M	L	M	M
L	M	L	H	M
L	M	M	L	M
L	M	M	M	M
L	M	M	H	M
L	M	H	L	M
L	M	H	M	M
L	M	H	H	H
M	L	L	L	I
M	L	L	M	L
M	L	L	H	M
M	L	M	L	M
M	L	M	M	M
M	L	M	H	M

CHANGE MANAGEMENT SEVERITY MATRIX				
Backout Effort	**Risk**	**Impact**	**Exposure**	**Severity**
M	L	H	L	M
M	L	H	M	M
M	L	H	H	H
M	M	L	L	M
M	M	L	M	M
M	M	L	H	M
M	M	M	L	M
M	M	M	M	M
M	M	M	H	H
M	M	H	L	M
M	M	H	M	H
M	M	H	H	H
M	H	L	L	M
M	H	L	M	M
M	H	L	H	H
M	H	M	L	M
M	H	M	M	H
M	H	M	H	H
M	H	H	L	H
M	H	H	M	H
M	H	H	H	H
H	L	L	L	M
H	L	L	M	M
H	L	L	H	H
H	L	M	L	M
H	L	M	M	M
H	L	M	H	H
H	L	H	L	H
H	L	H	M	H
H	L	H	H	H
H	M	L	L	M
H	M	L	M	H
H	M	L	H	H
H	M	M	L	H
H	M	M	M	H
H	M	M	H	H
H	M	H	L	H

CHANGE MANAGEMENT SEVERITY MATRIX				
Backout Effort	**Risk**	**Impact**	**Exposure**	**Severity**
H	M	H	M	H
H	M	H	H	H
H	H	L	L	H
H	H	L	M	H
H	H	L	H	H
H	H	M	L	H
H	H	M	M	H
H	H	M	H	H
H	H	H	L	H
H	H	H	M	H
H	H	H	H	H

The following tables will be used to determine the Backout Effort, Risk, Impact and Exposure of a Change:

Table 2. Determination of Backout Effort

	BACKOUT EFFORT		
Factors	LOW	MEDIUM	HIGH
Effort required to backout	Less than five minute outage	5-10 minute outage	More than 10 minute outage

Table 3. Determination of Impact

	IMPACT		
Factors	LOW	MEDIUM	HIGH
Impact to Service(s) during Change (partially) performed outside Change Window	None	Degradation	Outage
Impact to Service(s) if Change fails	None	Degradation	Outage
Implementers(s) on-site	Yes	Yes, with exposure or No, without exposure	No, with exposure

Table 4. Determination of Risk.

Factors	RISK		
	LOW	MEDIUM	HIGH
Testing performed prior to approval	Yes, extensive and satisfactory	Yes, minor and satisfactory or No, without exposure	Yes, inconclusive results or No, with exposure
Dependency on preceding or concurrent Change(s)	No	Yes, highest RISK of those changes is MEDIUM	Yes, highest RISK of those changes is HIGH
Unresolved resource conflict with preceding or concurrent Change(s)	No	Yes, highest RISK of those Changes is MEDIUM	Yes, highest RISK of those Changes is HIGH
Request for Province Staff and/or Service Provider Personnel	No	On-call or On-site	

Table 5. Determination of Exposure

Factor	RISK		
	LOW	MEDIUM	HIGH
The number of impacted Province Users, Client Organizations, Systems or subsystems (such as a shared database or a shared Application).	1-2 Province Users are impacted	Temporary outage to a few individuals	System, subsystem or Client Organization outage

Appendix J - Province Change Windows

The Change Windows are stated in terms of Pacific Time and are as follows:

1. "**General Change Window**" for Changes that may be disruptive:

S15

2. Authentication Services Change Window:

S15

3. Storage and Backup Services Change Window:

S15

4. Mainframe Change Windows:

Any Change to the mainframe production service that is disruptive or may be disruptive is scheduled in the General Change Window identified above.

The weekly system backups occur on S15

S15

For a service dedicated to a particular application, application owners can set their own Change Windows according to the following tables:

4.1 Multiple Virtual Storage ("MVS") Production Change Windows:

Application	Day of Week	Change Window
S15		

4.2 Multiple Virtual Storage ("MVS") Test Change Windows

Applications	Day of Week	Change Window
S15		

Applications	Day of Week	Change Window
S15		

5. Client Specific Change Windows

5.1 Unix Hosting Client Specific Change Windows

Client Organization	Day/Time
The following Client Organization specific Change Windows apply to specific Servers, initial notice of which will be provided to the Service Provider in the Manual following the Hand-Over Date.	
S15	

Pages 693 through 696 redacted for the following reasons:
- -
S15, S15

Appendix K – Change Management Entrance Criteria

The Change Management Process will apply when a Change:

(a) Is the installation of a new product or equipment.

(b) Is the de-installation of a product or equipment.

(c) Is the maintenance or upgrade of a product, service or equipment, or disruptive configuration change.

(d) Is a fix of a product, service or equipment.

(e) Is the testing of a product, service or equipment requiring resources or special operational instructions.

(f) Requires special operational procedures to be followed.

(g) Represents Requests for special processing consisting of extension of hours of operation, special jobs, special printouts and database re-organization.

(h) Amends procedures and documentation associated with the running and support of live systems.

(i) Is required to support a Change made outside the scope of the Services.

An RFC is <u>not</u> required for:

(a) Purely administrative activities such as adding an email ID or Organization Number where there is an existing audit trail in place.

(b) Any activity that is considered part of daily function and does not fall within the requirements listed above.

(c) No Change to configuration database.

Appendix L – Incident Prioritization Matrix

Priority 1

(a) "**Priority 1**" means a deficiency with a WTS service which has a critical impact on the Client Organization's business processes. Using a Work-around or manual process cannot reduce the impact.

(b) Context

- WTS, Province Partners and Service Provider supporting the impacted WTS service, and individuals in the Client Organization are expected to work continuously (24 x 7) until the Incident is resolved or until the Priority is reduced.

- All systems supporting Client Organization business processes that, if impacted, may result in a Priority 1 Incident, are expected to have 24 x 7 support.

Priority 2

(a) "**Priority 2**" means a deficiency with a WTS service which has a severe impact on the Client Organization's business processes. A limited Work-around or manual process is available.

(b) Context

- WTS, Province Partners and Service Provider supporting the impacted WTS service, and individuals in the Client Organization are expected to work during regular business hours until the Incident is resolved or the until Priority is reduced. However, if the systems supporting the Client Organization business process have 24 x 7 support, then all involved parties, including individuals in the Client Organization are expected to work continuously (24 x 7) until the Incident is resolved or until the priority is reduced.

- All systems supporting Client Organization business processes that require After Hours support are expected to have 24 x7 support.

Priority 3

(a) "**Priority 3**" means a deficiency with a WTS service which is not seriously impacting a Client Organization business processes. There may be a limited Work-around or manual process available that allows those impacted to achieve a level of service approaching normal service delivery during the event.

(b) Context

- WTS, Province Partners and Service Provider supporting the impacted WTS service, and individuals in the Client Organization are expected to continue working during regular business hours until the Incident is resolved.

Priority 4

(a) "**Priority 4**" means a deficiency with a WTS service which has a minor impact on a Client Organization's business processes and may include deficiencies impacting a single Province User.

(b) Context

- WTS, Province Partners and Service Provider supporting the impacted WTS service, and individuals in the Client Organization are expected to continue working during regular business hours until the Incident is resolved.

Priority 5

(a) "**Priority 5**" means an Incident used to track Problems within the Province Incident Management Application.

(b) Context

- Related Incidents are linked to Problems for tracking purposes.

Priority 6

(a) "**Priority 6**" means a Incident used to track Minor Service Requests within the Province Incident Management Application.

(b) Context

- Minor Service Requests are not orderable via Province Ordering System.

Appendix M – Significant Event Review

Purpose:

The following outlines the objectives and processes for a Significant Event Review.

WTS utilizes the Significant Event Review process to review the circumstances, actions, and adherence to process upon the occurrence of a Significant Event. A Significant Event may be a Change, series of Changes, an Incident, multiple Incidents (related to the same Client Organization or service) or a project. The review is initiated in order to document what occurred, understand where improvements can be realized and recommend actions to address failures or improve service.

This review takes the form of a meeting in which representatives from interested parties discuss the event. Following the meeting, a Significant Event Review document is drafted by the Change Management group. This document consists of a detailed summary of the discussions as well as the conclusions and recommendations reached at the meeting.

Objectives:

(a) To review and document significant technical events for the purpose improving services. Where applicable, identify Root Causes and make recommendations to prevent a reoccurrence and/or mitigate negative effects of similar events in the future.

(b) To encourage continuous technical service improvement.

Format:

SERs include the following information:

(a) Title (One sentence identifying the event).

(b) Review ID: Review number and associated Incident tickets, RFC.

(c) Attendees: including contributors.

(d) Description: One paragraph describing the event.

(e) Business Impact: a statement (usually provided by the customer) about how the Client Organization's business was impacted.

(f) Summary Timelines.

(g) Technical Findings: The key technical facts of the event.

(h) Process Findings: The key facts of the event including the adherence to established process consisting of Change process, Incident process, and communication process.

(i) Primary Root Cause: in one sentence, why the event happened where applicable.

(j) Recommendations: Specific actions to address Incident and future prevention.

(k) Service Improvement Opportunities: Specific actions for future prevention and/or improvement plans.

(l) Mitigation Measures: Any strategic action or activity that will reduce the likelihood or duration of a service disruption (e.g., develop a DRP, 24 X 7 coverage, change in technical architecture).

Significant Event Review Process relative to the Service Provider:

(a) The Significant Event Review process follows the completion of an event where it is deemed a review would be beneficial. (**Note**: the review could be requested by the Client Organization or internally if the event had a negative impact on Client Organization(s) or required attention by multiple groups).

(b) A request is made to the Service Provider for an internal review.

(c) A Significant Event Review meeting is held, interviews are conducted to gather facts related to the event, Root Cause and recommendations if applicable.

(d) A Significant Event Review document recording the discussions during the meeting is drafted following the meeting.

(e) The draft document is circulated among the attendees and interviewees for review and comments.

(f) The WTS Change Management group reviews the document and initiates revisions as may be necessary.

(g) The finalized document is filed and a copy is sent to the Significant Event Review meeting attendees, contributors and recommendation assignees.

(h) Recommendations and service improvement opportunities are logged and tracked for implementation.

Appendix N – Province Ordering System Request Lead Times

Lead times are targets and are measured in Business Days from the date of receipt of a Booked Order in the Province Ordering System.

ITEM	ITEM DESCRIPTION	TARGET DAYS
PI-ADDITIONAL SOFTWARE-FOR-MVS	Additional Software for MVS	20
PI-ADDITIONAL SOFTWARE-FOR-MVS-MONTHLY	Additional Software for MVS Monthly Rate	20
PI-ADDITIONAL SOFTWARE-FOR-MVS-ONE-TIME	Additional Software for MVS One Time Cost	20
PI-ADDITIONAL-SOFTWARE-FOR VMS	Additional Software for VMS	20
PI-ADDITIONAL-SOFTWARE-FOR-VMS-MONTHLY	Additional Software for VMS Monthly Charge	20
PI-ADDITIONAL-SOFTWARE-FOR-VMS-ONE-TIME	Additional Software for VMS One Time Cost	20
PI-APPL-HOSTING-SERVICE-FOR-UNIX-VIRT	Application Hosting Service for Virtual UNIX	30
PI-APPL-HOSTING-SERVICE-FOR-UNIX/LINUX	Application Hosting Service for UNIX/Linux	20
PI-APPL-HOSTING-SERVICE-FOR-WINDOWS	Application Hosting Service for Windows	20
PI-APPL-HOSTING-SERVICE-FOR-WINDWS-VIRT	Application Hosting Service for Virtual Windows	30
PI-APPL-HOSTING-SERVICE-FOR-UNIX/LINUX	Application Hosting Service for UNIX/Linux	20
PI-APPL-HOSTING-SERVICE-FOR-WINDOWS	Application Hosting Service for Windows	20
PI-APPLICATION-STORAGE-BUSINESS-PRIORITY	Tier 2 - Business Priority	20
PI-APPLICATION-STORAGE-GENERAL-BUSINESS	Tier 3 - General Business	20
PI-APPLICATION-STORAGE-MISSION-CRITICAL	Tier 1 - Mission Critical	40
PI-APPLICATION-STORAGE-STABLE/ARCHIVE	Tier 4 - Stable/Archive	20
PI-CANCEL-TIER1-MISSION-CRITICAL	Cancel Tier 1 Mission Critical	15
PI-CANCEL-TIER2-BUSINESS-PRIORITY	Cancel Tier 2 Business Priority	15
PI-CANCEL-TIER3-GENERAL-BUSINESS	Cancel Tier 3 General Business	15
PI-CANCEL-TIER4-STABLE/ARCHIVE	Cancel Tier 4 Stable/Archive	15
PI-DATA-MIRRORING-OR-REPLICATION	Data Mirroring or Replication	20
PI-DATA-MIRRORING-OR-REPLICATION-MONTHLY	Data Mirroring or Replication Monthly Rate	20
PI-DATA-MIRRORING-OR-REPLICATN-ONE-TIME	Data Mirroring or Replication One time Cost	20

ITEM	ITEM DESCRIPTION	TARGET DAYS
PI-CANCEL-APPLICATION-HOSTING-UNIX/LINUX	Cancel Application Hosting for UNIX/Linux	130
PI-CANCEL-APPLICATION-HOSTING-WINDOWS	Cancel Application Hosting for Windows	20
PI-CANCEL-ARCHIVAL-BACKUP	Cancel Archival Backup	66
PI-CANCEL-DATA-BACKUP-SERVICE	Cancel Data Backup Service	15
PI-CANCEL-DATA-MIRRORING-OR-REPLICATION	Cancel Data Mirroring or Replication	15
PI-CANCEL-HOSTING-SERVICES-ONE-TIME	Cancel Hosting Services One Time Cost	130
PI-CANCEL-SHARED-DATABASE-SERVICE	Cancel Shared Database Service	20
PI-CANCEL-SHARED-WEB-HOSTING-SERVICE	Cancel Shared Web Hosting Service	20
PI-CANCEL-SHAREPOINT-TEAM-COLLABORATION	Cancel SharePoint Team Collaboration	20
PI-CANCEL-TIER1-MISSION-CRITICAL	Cancel Tier 1 Mission Critical	15
PI-CANCEL-TIER2-BUSINESS-PRIORITY	Cancel Tier 2 Business Priority	15
PI-CANCEL-TIER3-GENERAL-BUSINESS	Cancel Tier 3 General Business	15
PI-CANCEL-TIER4-STABLE/ARCHIVE	Cancel Tier 4 Stable/Archive	15
PI-CANCEL-UNIX/LINUX-ADD-AGREEMENTS	Cancel UNIX/Linux Additional Agreements	130
PI-CANCEL-UNIX/LINUX-HARDWARE	Cancel UNIX/Linux Hardware	130
PI-CANCEL-UNIX/LINUX-SOFTWARE	Cancel UNIX/Linux Software	130
PI-CANCEL-UNIX/LINUX-SPECIAL-ASSEMBLY	Cancel UNIX/Linux Special Assembly	130
PI-CANCEL-WINDOWS-ADD-AGREEMENTS	Cancel Windows Additional Agreements	20
PI-CANCEL-WINDOWS-HARDWARE	Cancel Windows Hardware	20
PI-CANCEL-WINDOWS-SOFTWARE	Cancel Windows Software	20
PI-CANCEL-WINDOWS-SPECIAL-ASSEMBLY	Cancel Windows Special Assembly	20
PI-APPL-HOSTING-UNIX-CANCEL-COSTS	Application Hosting Service for UNIX/Linux - Cancellation Costs	130
PI-APPL-HOSTING-UNIX-VIRT-CANCEL-COSTS	Application Hosting Service for UNIX/Linux-Virtual - Cancellation Costs	130
PI-APPL-HOSTING-WIN-VIRT-CANCEL-COSTS	Application Hosting Service for Windows - Virtual - Cancellation Costs	130
PI-APPL-HOSTING-WINDOWS-CANCEL-COSTS	Application Hosting Service for Windows - Cancellation Costs	130
PI-APPLICATION-STORAGE-CANCEL-COSTS	Application Storage Services - Cancellation Costs	15
PI-DATA-MIRRORING-CANCEL-COSTS	Data Mirroring - Cancellation Costs	130
PI-HW-SUPPORT-AGREEMENT-CANCEL-COSTS	Support Agreement Cancellation Costs	30

ITEM	ITEM DESCRIPTION	TARGET DAYS
PI-OPEN-VMS-CANCELLATION-COSTS	OpenVMS Cancellation Costs	30
PI-SHARED-DATABASE-CANCEL-COSTS	Shared Database Service - Cancellation Costs	130
PI-SHARED-WEB-CANCEL-COSTS	Shared Web Hosting Service - Cancellation Costs	130
PI-SHAREPOINT-CANCEL-COSTS	SharePoint Team Collaboration - Cancellation Costs	130
PI-UNIX-HARDWARE-NEW-CANCEL-COSTS	UNIX Hardware New Cancellation Costs	130
PI-UNIX-HARDWARE-UPGRADE-CANCEL-COSTS	UNIX Hardware Upgrade Cancellation Costs	130
PI-WINDOWS-HARDWARE-NEW-CANCEL-COSTS	Windows Hardware New Cancellation Costs	130
PI-WINDOWS-HARDWARE-UPGRADE-CANCEL-COSTS	Windows Hardware Upgrade Cancellation Costs	130
PI-ARCHIVAL BACKUP	Archival Backup	10
PI-DATA BACKUP SERVICE	Data Backup Services	8
PI-DATA-MIRRORING-OR-REPLICATION	Data Mirroring or Replication	20
PI-DATA-MIRRORING-OR-REPLICATION-MONTHLY	Data Mirroring or Replication Monthly Rate	20
PI-DATA-MIRRORING-OR-REPLICATN-ONE-TIME	Data Mirroring or Replication One time Cost	20
PI-DEDICATED-SFP-SERVER	Dedicated SFP Server	20
PI-DEDICATED-SFP-SERVER-MONTHLY	Dedicated SFP Server - Monthly Cost	20
PI-DEDICATED-SFP-SERVER-ONE-TIME	Dedicated SFP Server - One Time Cost	20
PI-HOSTING-HW-SUPPORT-AGREEMENT	Hosting Hardware Support Agreement	30
PI-HOSTING-HW-SUPPORTAGREEMENT-MTH	Hosting Hardware Support Agreement - Monthly	30
PI-HOSTING-HW-SUPPORTAGRMENT-ONE	Hosting Hardware Support Agreement - One Time	30
PI-HOSTING-UNIX-LINUX-HW-NEW-MONTHLY	New UNIX-Linux Hardware - Monthly Costs	20
PI-HOSTING-UNIX-LINUX-HW-NEW-ONE-TIME	New UNIX-Linux Hardware - One Time Cost	20
PI-HOSTING-UNIX-LINUX-HW-UPGRADE-MONTHLY	UNIX-Linux Hardware Upgrade-Monthly Costs	20
PI-HOSTING-UNIX-LINUX-HW-UPGRADE-ONETIME	UNIX-Linux Hardware Upgrade-One Time Cost	20
PI-HOSTING-UNIX-LINUX-HWNEW	New UNIX-Linux Hardware	20
PI-HOSTING-UNIX-LINUX-HWUPGRADE	UNIX-Linux Hardware Upgrade	20
PI-HOSTING-WINDOW-HW-NEW-MONTHLY	New Windows Hardware - Monthly Costs	20

ITEM	ITEM DESCRIPTION	TARGET DAYS
PI-HOSTING-WINDOW-HW-NEW-ONE-TIME	New Windows Hardware - One Time Cost	20
PI-HOSTING-WINDOW-HW-UPGRADE-MONTHLY	Windows-Hardware Upgrade - Monthly Costs	20
PI-HOSTING-WINDOW-HW-UPGRADE-ONE-TIME	Windows Hardware Upgrade - One Time Cost	20
PI-HOSTING-WINDOW-HWNEW	New Windows Hardware	20
PI-HOSTING-WINDOW-HWUPGRADE	Windows-Hardware Upgrade	20
PI-ADMINISTRATIVE-SUPPORT-HOSTING	Administrative Support Consulting Services - Hosting	14
PI-ANALYST-HOSTING	Analyst Consulting Services - Hosting	14
PI-HOSTING-CONSULTING-MULTIPLEREQUESTS	Hosting Consulting Service - Multiple Request Quote	14
PI-HOSTING-CONSULTING-SERVICES	Hosting Services - Consulting	14
PI-HOSTING-CONSULTING-SINGLEREQUEST	Hosting Consulting Service - Single Request Quote	14
PI-INTERMEDIATE-ANALYST-HOSTING	Intermediate Analyst Consulting Services-Hosting	14
PI-MANAGEMENT-HOSTING	Management Consulting Services - Hosting	14
PI-SENIOR-ANALYST-HOSTING	Senior Analyst Consulting Services - Hosting	14
PI-TECHNICAL-SPECIALIST-HOSTING	Technical Specialist Consulting Services - Hosting	14
PI-OPEN-VMS SERVICE	OpenVMS Service	30
PI-OPEN-VMS-SERVICE-MONTHLY	OpenVMS Service - Monthly Charge	30
PI-OPEN-VMS-SERVICE-ONE-TIME	OpenVMS Service - One-Time Cost	30
PI-SFP-ENHANCED-AUDITING-MONTHLY	SFP Enhanced Auditing Service - Monthly	20
PI-SFP-ENHANCED-AUDITING-ONE-TIME	SFP Enhanced Auditing Service - One-Time	20
PI-SFP-ENHANCED-AUDITING-SERVICE	SFP Enhanced Auditing Service	20
PI-SHARED-DATABASE-SERVICES	Shared Database Services	10
PI-SHARED-WEB-HOSTING-SERVICE	Shared Web Hosting Service	3
PI-SHARED-WEB-HOSTING-UNIX-DYNAMIC-DEV	Shared Web Hosting - UNIX Dynamic Development Site	3
PI-SHARED-WEB-HOSTING-UNIX-DYNAMIC-PROD	Shared Web Hosting - UNIX Dynamic Production Site	3
PI-SHARED-WEB-HOSTING-UNIX-DYNAMIC-TEST	Shared Web Hosting - UNIX Dynamic Test Site	3
PI-SHARED-WEB-HOSTING-UNIX-STATIC-DEV	Shared Web Hosting - UNIX Static Development Site	3
PI-SHARED-WEB-HOSTING-UNIX-STATIC-PROD	Shared Web Hosting - UNIX Static Production Site	3
PI-SHARED-WEB-HOSTING-UNIX-STATIC-TEST	Shared Web Hosting - UNIX Static Test Site	3
PI-SHARED-WEB-HOSTING-WIN-	Shared Web Hosting - Windows Dynamic	3

ITEM	ITEM DESCRIPTION	TARGET DAYS
DYNAMIC-DEV	Development Site	
PI-SHARED-WEB-HOSTING-WIN-DYNAMIC-PROD	Shared Web Hosting - Windows Dynamic Production Site	3
PI-SHARED-WEB-HOSTING-WIN-DYNAMIC-TEST	Shared Web Hosting - Windows Dynamic Test Site	3
PI-SHARED-WEB-HOSTING-WIN-STATIC-DEV	Shared Web Hosting - Windows Static Development Site	3
PI-SHARED-WEB-HOSTING-WIN-STATIC-PROD	Shared Web Hosting - Windows Static Production Site	3
PI-SHARED-WEB-HOSTING-WIN-STATIC-TEST	Shared Web Hosting - Windows Static Test Site	3
PI-UNIX/LINUX-HARDWARE/SOFTWARE/AGRMNTS	UNIX/Linux Hardware, Software or Additional Agreements	20
PI-UNIX/LINUX-HW/SW-HARDWARE-ONE-TIME	UNIX/LINUX Hardware One Time Cost	20
PI-UNIX/LINUX-HW/SW-SOFTWARE-ONE-TIME	UNIX/LINUX Hardware One Time Cost	20
PI-UNIX/LINUX-HW/SW/AGRMNTS-AGREEMENTS	UNIX/Linux Additional Agreements	44
PI-UNIX/LINUX-HW/SW/AGRMNTS-HARDWARE	UNIX/Linux Hardware Monthly Cost	20
PI-UNIX/LINUX-HW/SW/AGRMNTS-SOFTWARE	UNIX/Linux Software Monthly Cost	20
PI-UNIX/LINUX-SPECIAL-ASSEMBLY	Unix/Linux Special Assembly	44
PI-UNIX/LINUX-SPECIAL-ASSEMBLY-MONTHLY	Unix/Linux Special Assembly Monthly Rate	44
PI-UNIX/LINUX-SPECIAL-ASSEMBLY-ONE-TIME	Unix/Linux Special Assembly One Time Cost	44
PI-WINDOWS-HARDWARE/SOFTWARE/AGRMNTS	Windows Hardware, Software or Additional Agreements	20
PI-WINDOWS-HW/SW-HARDWARE-ONE-TIME	Windows Hardware One Time Cost	20
PI-WINDOWS-HW/SW-SOFTWARE-ONE-TIME	Windows Software One Time Cost	20
PI-WINDOWS-HW/SW/AGRMNTS-AGREEMENTS	Windows Additional Agreements	20
PI-WINDOWS-HW/SW/AGRMNTS-HARDWARE	Windows Hardware Monthly Cost	20
PI-WINDOWS-HW/SW/AGRMNTS-SOFTWARE	Windows Software Monthly Cost	20
PI-WINDOWS-SPECIAL-ASSEMBLY	Windows Special Assembly	44
PI-WINDOWS-SPECIAL-ASSEMBLY-MONTHLY	Windows Special Assembly Monthly Rate	44
PI-WINDOWS-SPECIAL-ASSEMBLY-ONE-TIME	Windows Special Assembly One Time Cost	44
PI-CANCEL-APPLICATION-HOSTING-UNIX-VIRT	Cancel Application Hosting for UNIX/Linux - Virtual	130

ITEM	ITEM DESCRIPTION	TARGET DAYS
PI-CANCEL-APPLICATION-HOSTING-UNIX/LINUX	Cancel Application Hosting for UNIX/Linux	130
PI-CANCEL-APPLICATION-HOSTING-WIN-VIRT	Cancel Application Hosting for Windows - Virtual	20
PI-CANCEL-APPLICATION-HOSTING-WINDOWS	Cancel Application Hosting for Windows	20
PI-CANCEL-DATA-MIRRORING-OR-REPLICATION	Cancel Data Mirroring or Replication	15
PI-CANCEL-HOSTING-HW-SUPPORT-AGREEMENT	Hosting Hardware Support Agreement - Cancel	30
PI-CANCEL-HOSTING-HW-SUPPORTAGREEMENT	Hosting Hardware Support Agreement - Cancel	30
PI-CANCEL-HOSTING-SERVICES-ONE-TIME	Cancel Hosting Services One Time Cost	130
PI-CANCEL-OPEN-VMS-SERVICE	Cancel OpenVMS Service	30
PI-CANCEL-SHARED-DATABASE-SERVICE	Cancel Shared Database Service	20
PI-CANCEL-SHARED-WEB-HOSTING-SERVICE	Cancel Shared Web Hosting Service	20
PI-CANCEL-SHARED-WEB-UNIX-DYNAMIC-DEV	Cancel Shared Web Hosting Service - UNIX Dynamic Development	20
PI-CANCEL-SHARED-WEB-UNIX-DYNAMIC-PROD	Cancel Shared Web Hosting Service - UNIX Dynamic Production	20
PI-CANCEL-SHARED-WEB-UNIX-DYNAMIC-TEST	Cancel Shared Web Hosting Service - UNIX Dynamic Test	20
PI-CANCEL-SHARED-WEB-UNIX-STATIC-DEV	Cancel Shared Web Hosting Service - UNIX Static Development	20
PI-CANCEL-SHARED-WEB-UNIX-STATIC-PROD	Cancel Shared Web Hosting Service - UNIX Static Production	20
PI-CANCEL-SHARED-WEB-UNIX-STATIC-TEST	Cancel Shared Web Hosting Service - UNIX Static Test	20
PI-CANCEL-SHARED-WEB-WIN-DYNAMIC-DEV	Cancel Shared Web Hosting Service - Windows Dynamic Development	20
PI-CANCEL-SHARED-WEB-WIN-DYNAMIC-PROD	Cancel Shared Web Hosting Service - Windows Dynamic Production	20
PI-CANCEL-SHARED-WEB-WIN-DYNAMIC-TEST	Cancel Shared Web Hosting Service - Windows Dynamic Test	20
PI-CANCEL-SHARED-WEB-WIN-STATIC-DEV	Cancel Shared Web Hosting Service - Windows Static Development	20
PI-CANCEL-SHARED-WEB-WIN-STATIC-PROD	Cancel Shared Web Hosting Service - Windows Static Production	20
PI-CANCEL-SHARED-WEB-WIN-STATIC-TEST	Cancel Shared Web Hosting Service - Windows Static Test	20
PI-CANCEL-SHAREPOINT-TEAM-COLLABORATION	Cancel SharePoint Team Collaboration	20
PI-CANCEL-TIER1-MISSION-CRITICAL	Cancel Tier 1 Mission Critical	15
PI-CANCEL-TIER2-BUSINESS-	Cancel Tier 2 Business Priority	15

ITEM	ITEM DESCRIPTION	TARGET DAYS
PRIORITY		
PI-CANCEL-TIER3-GENERAL-BUSINESS	Cancel Tier 3 General Business	15
PI-CANCEL-TIER4-STABLE/ARCHIVE	Cancel Tier 4 Stable/Archive	15
PI-CANCEL-UNIX-HARDWARE-NEW	Cancel UNIX Hardware New	20
PI-CANCEL-UNIX-HARDWARE-UPGRADE	Cancel UNIX Hardware Upgrade	20
PI-CANCEL-UNIX/LINUX-ADD-AGREEMENTS	Cancel UNIX/Linux Additional Agreements	130
PI-CANCEL-UNIX/LINUX-HARDWARE	Cancel UNIX/Linux Hardware	130
PI-CANCEL-UNIX/LINUX-SOFTWARE	Cancel UNIX/Linux Software	130
PI-CANCEL-UNIX/LINUX-SPECIAL-ASSEMBLY	Cancel UNIX/Linux Special Assembly	130
PI-CANCEL-WINDOWS-ADD-AGREEMENTS	Cancel Windows Additional Agreements	20
PI-CANCEL-WINDOWS-HARDWARE	Cancel Windows Hardware	20
PI-CANCEL-WINDOWS-HARDWARE-NEW	Cancel Windows Hardware New	20
PI-CANCEL-WINDOWS-HARDWARE-UPGRADE	Cancel Windows Hardware Upgrade	20
PI-CANCEL-WINDOWS-SOFTWARE	Cancel Windows Software	20
PI-CANCEL-WINDOWS-SPECIAL-ASSEMBLY	Cancel Windows Special Assembly	20
PI-APPL-HOSTING-UNIX/LINUX-BASE	Appl. Hosting Service for UNIX/Linux Baseline	N/A
PI-APPL-HOSTING-UNIX/LINUX-FRCST	Appl. Hosting Service for UNIX/Linux Forecast	N/A
PI-APPL-HOSTING-WINDOWS-BASE	Appl. Hosting Service for Windows Baseline	N/A
PI-APPL-HOSTING-WINDOWS-FRCST	Appl. Hosting Service for Windows Forecast	N/A
PI-CANCEL-DEDICATED-SFP-SERVER	Dedicated SFP Server - Cancel	20
PI-DATA-BACKUP-SERVICE-BASE	Data Backup Service Baseline	N/A
PI-DATA-BACKUP-SERVICE-FRCST	Data Backup Service Forecast	N/A
PI-DEDICATED SERVER-ONE-TIME	Dedicated Server	20
PI-DEDICATED-SERVER-MONTHLY	Dedicated Server	20
PI-INCREMENTAL-MGD-STORAGE-SHARED-WEB	Incremental Managed Storage (Shared Web)	14
PI-INCREMENTAL-MGD-STORAGE-SHAREPOINT	Incremental Managed Storage (SharePoint)	14
PI-INCREMNTL-MGD-STORAGE-SHARED-DATABASE	Incremental Managed Storage (Shared Database)	14
PI-MAINFRAME-SERVICES-(MVS)	Mainframe Services (MVS)	N/A
PI-OPENVMS-SERVICE-CONSUMPTION	OpenVMS Unit Based	N/A
PI-OPENVMS-SERVICES-MONTHLY	OpenVMS Windows Service Rate	N/A
PI-SHARED-DATABASE-SERVICES-BASE	Shared Database Service Baseline	N/A

ITEM	ITEM DESCRIPTION	TARGET DAYS
PI-SHARED-DATABASE-SERVICES-FRCST	Shared Database Service Forecast	N/A
PI-UNIX/LINUX OR WINDOWS SW PASSTRHU	Unix/Linux or Windows Software - Pass Through	20

Appendix O – Province Reports

Name	
S. 15	

Name	
S. 15	
WTS Current incident reporting available for P1's – P4's: • Acceptance. • Update. • Resolution. • Reporting is done by Assignment group based on Priority using the Priority level. Incident details are available at the beginning of each summary. S. 15	

Appendix P – TIBs Guidelines

PUBLISHING GUIDELINES FOR
WTS TECHNICAL INFORMATION BULLETINS
(September 2003)

Overview

A TIB provides details on any changes to the Supported Infrastructure, extended outages or processes. This includes upgrades to product versions, retirement of products, availability of new products, and any other activity that will impact customers or require some form of customer action, such as testing, JCL changes, and so on. It is mandatory that a TIB be prepared for all changes impacting Client Organizations PRIOR to the implementation of the activity.

Once the TIB has been approved, it is published by the Province to inform Client Organizations and other interested parties of these changes.

TIBs apply to changes on MVS, VM, NT, GEMS, OPENVMS, UNIX, ENVIRONMENT and NETWORK environments.

TIME FRAME FOR PREPARATION, REVIEW, APPROVAL AND PUBLICATION OF TIBs

TIBs are to be prepared in advance to allow adequate time for review, revisions, approval and publication. The following table provides lead times on the publication of TIBs depending on the nature of the activity.

Type of Activity	Risk/Impact	Notice to Customers	Review / Approval
Customer Action Required: • Operation procedures • JCL • Documentation	Low	28 days	35 days
Components (programs, screens, etc.)	High	up to 60 days	+7 days
SPIN	High	90 days	
Decrease in Service Stability	Low <=1 hr	14 days	21 days
Degradation of performance	High=>1 hr	28 days	35 days
Information Only	None	None	None
• New Product Announcement • Reminder of previously published TIB • Emergency TIBs (events that can't be	Note 1	Note 1	Note 1

Type of Activity	Risk/Impact	Notice to Customers	Review / Approval
predicted)			
• Product Retirement	Low Volume High Volume	1 year 2 years	

*Note 1: Although there is no specified lead time, the greater the customer impact, the longer the lead time should be.

IMPORTANT: If the activity described in a TIB requires an RFC, the RFC MUST be submitted prior to the publication of the TIB.

EMERGENCY TIBs

For TIBs requiring immediate publication, please contact the WTS Technical Change Management Group at (250) 387-8058 or (250) 387-8077, or send an email note to WTSTIBS@GEMS1.GOV.BC.CA.

CREATION OF TIBs

Roles and Responsibilities

TIB Originator - The creation of TIBs is the responsibility of the area delivering the service or implementing the change. See the PROCEDURES FOR CREATING A TIB section below for instructions on how to prepare a TIB.

TIB Editor - The TIB Editor (WTS Change Management Group) will review TIBs for grammar and spelling accuracy; overall formatting, layout and consistency of TIB; restructure paragraphs, provide recommendations for additional information to be included in the TIB, and ensure that the TIB is written with a customer perspective in mind. Additional information to be added will be the responsibility of the TIB originator.

PROCEDURES FOR CREATING A TIB

TIBs are prepared in the WTS WEB environment. WTS Change Management maintains the administrative functions for TIB creation, review, and approval privileges for all Ids recorded in the system. If you do not have Create A New TIB as a selection option after accessing the WTS web page noted below, and you must submit a TIB into the system, please contact the Change Management group via the Email ID WTSTIBS@GEMS1.GOV.BC.CA.

1. To access the WTS Technical Information web page go the following web location and select Technical Information Bulletins:
   https://WTS.gov.bc.ca/cust/Menu/Technical_Info.htm

2. Select Create A New TIB. You will be brought to a static TIB creation page where submitters are presented with a form containing ten fields, some noted below for data

entry. Submitters also have the option to copy an existing TIB if the activity closely resembles a known TIB in the database therefore allowing submitters to create a new TIB using data from a previously published TIB

3. Use the brief descriptions below as a guideline for entering data into the fields of a TIB:

   - Publication Date - Should be a Thursday at least 10 days after the date the TIB is submitted for processing.

   - Subject - Include subject of activity.

   - Activity - Include effective implementation date, activity and reason for activity.

   - Customer Impact - List all customer impact items. Encourage testing, if appropriate. Include brief instructions for testing and/or refer reader to TESTING PROCEDURES SECTION for more details. The Customer Impact section should summarize what action is required of the Client Organization.

   - Description - Provide overview of the activity. Include what changes are being implemented, in detail. If detail is large, refer readers to a separate location containing the details.

   - Testing Procedures - If testing is required by Client Organizations, state the date and time of test slots. Include details of the test script' here.

   - Documentation - Include manuals, on-line information, links to other sites, and other sources. Advise Client Organizations where the information is available and how to obtain it.

4. Once all fields have been updated use the SUBMIT option and a new TIB number will be presented to the submitter. This will promote the TIB to the review and publication phases of the process.

APPROVAL PROCESS

TIBs reviewers, technical managers and analysts, service managers, WTS Customer Support Representatives, Customer Service Centre, and WTS Communications Group are asked to ensure that TIBs are technically accurate and written in a clear, complete and concise manner by selecting the REVIEW UNPUBLISHED TIBs selection. Reviewers will already have been sent an email notification making them aware new TIBs for review. Comments can be made directly by selecting the Add A Review option at the top of the draft TIB being viewed.

To obtain access to review new TIBs for publication please contact the WTS Change Management group at WTSTIBS@GEMS1.GOV.BC.CA

Note: To ensure that a TIB be reviewed and published in a timely manner, TIBs must be completed and submitted no later than Friday at 12 noon. If approved, TIBs are published the following Thursday/Friday of each week.

Service Stability Control Group (SSCG)

TIBs are reviewed and approved by the Service Stability Control Group (SSCG) every Thursday morning. The Groups consists of staff from:

- WTS Technical Change Management Group
- WTS Network Technical Support
- WTS Service Centre
- TELUS Management
- Customer Support Representatives Group
- WTS Security Services

TIB Originators may be required to attend this meeting and reply to any recommended changes to the TIB in conjunction with TIB reviewers. If changes are minimal, the TIB will be published on the Thursday or Friday. If major changes are to be made to the TIB, it will be necessary to repeat the review process the following week.

PUBLICATION OF TIBs

Once a TIB has been reviewed and approved by SSCG, the TIB will be published to the WTS website at: https://WTS.gov.bc.ca/cust/menu/technical_info.htm

TIB RESOURCES

WTS Technical Change Management Group

See Authorization Matrix

STMS Hosting Services

SOW 8 – Business Continuity and Disaster Recovery Services

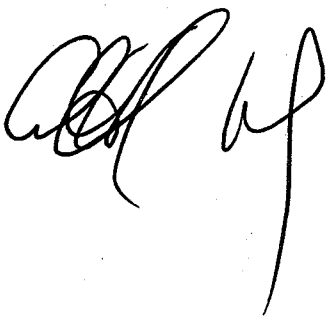


TABLE OF CONTENTS

1. SOW 8 - SUMMARY AND SCOPE OF SERVICES

1.1 Definitions

Capitalized terms used in this Statement of Work ("SOW") that are not defined within this SOW shall incorporate the meanings given to such words in the Agreement. In the event that a term is not defined in the Agreement, it shall have the meaning provided in Appendix A of this SOW or in the body of this SOW.

1.2 Purpose of this Document

1.2.1 Purpose of this Document

The purpose of this SOW is to describe, in detail, the scope and functions of the Business Continuity and Disaster Recovery Services to be provided by Service Provider to the Province and any Client under the terms of the Agreement.

1.2.2 Components of the Business Continuity and Disaster Recovery Services – Overview

The components of the Business Continuity and Disaster Recovery Services are set forth below:

(a) Assumption by Service Provider of Responsibility for Managing the Continuity of the Services – Overview

The assumption of responsibility for the Province's Business Continuity Plans and Disaster Recovery Plans applicable to the Services comprise the following components, which are more particularly described in Section 2 (*Assumption by Service Provider of Responsibility for Managing the Continuity of the Services*) set out below:

- Before Hand-Over Date
- On Hand-Over Date
- After Hand-Over Date

(b) Continuity Enablers in the Solution – Overview

Continuity Enablers are those modular services and technologies that the Service Provider has developed to offer Disaster Recovery Services to the Province and any Client. The Continuity Enablers available from the Service Provider's service catalogue comprise the following service components, which are more particularly described in Section 3 (*Continuity Enablers in the Solution*) set out below:

- Business Continuity Plan and Disaster Recovery Plan Development
- Service Catalogue Offerings for Continuity of Services

- Service Catalogue Disaster Recovery Reserve Units
- Disaster Recovery Measures to Achieve Recovery Time Objectives between 24 and 72 Hours
- Disaster Recovery Measures to Achieve Recovery Time Objectives between 4 and 24 Hours
- Geographically Dispersed Cluster Offerings With Very High Service Level Commitments for Applications that Require Recovery Time Objectives of Less Than 4 Hours

(c) Future Business Continuity Plan and Disaster Recovery Opportunities – Overview

Service Provider's vision of possible future Business Continuity and Disaster Recovery Service opportunities is more particularly described in Section 4 (*Future Business Continuity Plan and Disaster Recovery Opportunities*) set out below.

1.2.3 Appendices

The following Appendices are attached to and form part of this SOW:

- Appendix A – Definitions
- Appendix B – Reports
- Appendix C – Service Provider Efforts
- Appendix D – Mainframe Disaster Recovery Services
- Appendix E – Sample SOW for DRP

1.3 Use of RASIC Tables

The RASIC tables in this Statement of Work set forth the roles and responsibilities of the Service Provider and the Province for specific service elements within a service component. The RASIC tables are populated with responsibility indicators as follows:

Responsible: solely and directly accountable for creating a work product or otherwise for completing the task or responsibility identified

Approving: needs to review and assure such work product's quality

Supporting: any and all individuals or groups who help to create such work product

Informed: any and all who need updates during the creation of such work product or during the execution of a business process

Consulted: any and all who help define product design or quality review criteria

1.4 Common Services

This Statement of Work may contain references to services, activities, procedures or responsibilities that are more particularly defined in other Statements of Work, which are attached to the Agreement and are incorporated into the Agreement, including the Transformation SOW.

2. ASSUMPTION BY SERVICE PROVIDER OF RESPONSIBILITY FOR MANAGING THE CONTINUITY OF THE SERVICES

The purpose of this section is to describe in detail the manner in which the Service Provider will assume responsibility for managing the continuity of the Services to be provided by the Service Provider.

The Service Provider's Business Continuity Plan(s) (the "**Service Provider BCP**") deal with the Service Provider's ability to continue internal business operations impacted by any business disruption. All obligations, including development, maintenance, approval and exercise of the Service Provider BCPs are the responsibility of, and are provided by, the Service Provider in support of the Services.

The Service Provider's Disaster Recovery Plan(s) (the "**Service Provider Disaster Recovery Plan(s)**") deal with the recovery and restoration of the Services. Updates, maintenance, approval and annual exercise of the Service Provider Disaster Recovery Plans are the responsibility of, and provided by, the Service Provider in support of the Services.

The scope of these plans is limited to the Services of the Service Provider and they are not intended to replace the need for Province to have Business Continuity and Disaster Recovery Plans for their own business services, applications and operations. Notwithstanding anything to the contrary that may be contained in the Agreement, the Province and the Service Provider have agreed that it will not be necessary for the Province to approve the Service Provider's Business Continuity Plan(s).

2.1 Before Hand-Over Date

The Service Provider will prepare its initial Business Continuity Plan ("**BCP**") in respect of the Services, before the expected Hand-Over Date.

The Service Provider BCP will expressly address Force Majeure Events and Labour Disruptions.

Notwithstanding the protection by copyright and intellectual property rights of existing WTS BCP templates and documentation, the Service Provider BCP will include elements similar to those in the WTS BCP that is expected to be in effect at the Hand-Over Date. The Parties acknowledge that in the event of a Disaster occurring immediately after the Hand-Over Date and until the Transitioning Employees transition into the Service Provider Office Facilities (as those terms are defined in Schedule 9 (*Transformation*)), the Service Provider will recover the Services using the Transitioning Employees at the WTS Office Facilities (as defined in Schedule 9 (*Transformation*)) using the work processes used by the Province immediately prior to the Hand-Over Date.

The Service Provider has relied on the following listed WTS BCPs as a reference for developing some elements of the Service Provider BCP:

(a) Windows Hosting_12 section2_business_unit_single_section_no_rollup v4 - redacted).pdf

(b) 12 section2_business_unit_upd_single_section_no_rollup open vms.pdf

(c) 12 section2_business_unit_upd_single_section_no_rollup enterprise backup(2).pdf

(d) 12 section2 2_business_unit_rollup(2) OSG.pdf

The following table lists the respective responsibilities of the Province and the Service Provider applicable to the period which is prior to the Hand-Over Date.

Before Hand-Over Date	Responsibility	
	Province	Service Provider
Provide the Province a "Service Provider Business Continuity Representative" and alternate representative(s) as appropriate, including all contact information specifics.		R
Provide the Service Provider a "Province Business Continuity Representative" and alternate representative(s) as appropriate, including all contact information specifics.	R	
Notify the Province and any Client, as applicable, in writing, within 3 Business Days of the relevant change, when the "Service Provider Business Continuity Representative" or alternate(s) change, or when contact information specifics change.		R
Notify the Service Provider, in writing, within 3 Business Days of the relevant change, when the "Customer Business Continuity Representative" or alternate(s) change, or when contact information specifics change.	R	
Act as liaison with the Province to coordinate and ensure the integration of Service Provider BCP with those of the Province.		R
Confirm WTS Recovery Time Objective ("**RTO**") commitments, capacity to deliver, in-scope BCPs and Disaster Recovery Plans, and most recent Recovery Exercise report for each Disaster Recovery Plan.	R	

Before Hand-Over Date	Responsibility	
	Province	Service Provider
Provide to Service Provider, in writing, WTS RTO commitments, capacity to deliver, disclosure of in-scope BCPs and Disaster Recovery Plans, and most recent Recovery Exercise report for each Disaster Recovery Plan, all of which have been confirmed by the Province.	R	
Include in the Service Provider BCP actions to be taken in response to Force Majeure Events where such actions are expected to be effective to support the recovery of Services disrupted by such Force Majeure Events and to support the activation and execution of the Service Provider Disaster Recovery Plan(s).		R
If the available recovery actions documented in the Service Provider BCP are determined to be ineffective for the restoration of Services that are disrupted by a Force Majeure Event, then identify in the Service Provider BCP the prudent and commercially reasonable efforts that will be taken in cooperation with the Province and any Client, as applicable, in support of restoration of Services that are requested by the Province or a Client as described in Appendix C (*Service Provider Efforts*).		R
Create the Service Provider BCP for the support of the Services.		R
Provide written confirmation to the Province that the Service Provider has developed its initial BCP for supporting the Services and that the plan(s) have been reviewed and approved by senior Service Provider management.		R

Before Hand-Over Date	Responsibility	
	Province	Service Provider
Include in the Service Provider BCP a Labour Disruption Plan which includes and stipulates that: • the Province and any Client, as applicable, will be immediately notified by the Service Provider of the anticipation of, or the existence of, a Labour Disruption event which affects or may potentially affect the Services; • a daily status and impact update will be provided to the Province and any Client with respect to such event; • , in the event of a Labour Disruption, the Service Provider will use commercially reasonable efforts to carry on the Services on an uninterrupted basis through the application of management level Personnel and other staff that may be available or recruited; and • the Service Provider may will seek available remedies, such as injunctive or such other relief as may be deemed necessary or appropriate in the circumstances, in order to maintain access to any service locations that require the presence of Service Provider Personnel.		R

2.2 On Hand-Over Date

The Service Provider will update its initial BCP in respect of the Services, on the Hand-Over Date, as follows.

On Hand-Over Date	Responsibility	
	Province	Service Provider
Update the initial Service Provider BCP with appropriate personal information and any other information as may be required or deemed necessary by the Service Provider to enable the effective implementation and activation of the Service Provider BCP.		R
Distribute to the appropriate Service Provider Personnel and responders the updated Business Continuity Plan(s).		R
Provide written confirmation to the Province that the Service Provider has distributed the updated initial Service Provider BCP to the appropriate Service Provider Personnel and responders supporting the Services.		R

2.3 After Hand-Over Date

Service Provider will perform an acceptance process for the Service Provider's role in existing in-scope Disaster Recovery Plans based on their most recent documented Recovery Exercise results as disclosed by the Province prior to the Hand-Over Date.

2.3.1 Acceptance of Previously Exercised Plans

During the first month following the Hand-Over Date, Service Provider and Province will jointly review the results of the most recent Recovery Exercise with respect to those previously exercised in-scope Disaster Recovery Plans listed below in this Section 2.3.1 (*Acceptance of Previously Exercised Plans*). The purpose of this review is to initially identify any gaps or issues relating to the anticipated effectiveness of the Service Provider's tasks set out in these Disaster Recovery Plans.

The following table lists the respective responsibilities of the Province and the Service Provider applicable to the period which follows the Hand-Over Date.

After Hand-Over Date	Responsibility	
	Province	Service Provider
Develop and maintain a list of approved Service Provider Disaster Recovery Plans which support the restoration and recovery of the Services, including approval dates, a record of amendments, and exercise log.		R
During the first two months following the Hand-Over Date, review jointly with the Province the results of the most recent Recovery Exercise for in-scope Disaster Recovery Plans, which occurred prior to the Hand-Over Date.		R
During the first two months following the Hand-Over Date, review jointly with the Service Provider, the results of the most recent Recovery Exercise for in-scope Disaster Recovery Plans, which occurred prior to the Hand-Over Date.	R	
During the first two months following the Hand-Over Date, determine, and inform the Service Provider in writing, whether the Recovery Exercise achieved the Province's business objectives for RTO as defined in the Disaster Recovery Plan.	R	
Accept and add the Disaster Recovery Plan to the list of approved Service Provider Disaster Recovery Plans, if the most recent Recovery Exercise is determined and advised in writing by the Province to have achieved the Province's business objectives for RTO as defined in the Disaster Recovery Plan.		R

After Hand-Over Date	Responsibility	
	Province	Service Provider
If the Recovery Exercise does not achieve the Province's business objectives for RTO as defined in the Disaster Recovery Plan, update the Disaster Recovery Plan, but not insofar as including a change in assets or the services of a third party supplier.		R
If the test Recovery Exercise does not achieve the Province's business objectives for RTO as defined in the Disaster Recovery Plan and additional assets or the services of a third party supplier are required, propose a change to the Disaster Recovery Plan. Such change to be effected in accordance with the Governance Process or through the Change Order Process, as applicable, pursuant to the provisions set out in the Agreement.		R
Accept and add the Disaster Recovery Plan to the list of Service Provider Disaster Recovery Plans if the Disaster Recovery Plan has been effected in accordance with the Governance Process or through the Change Order Process, as applicable, pursuant to the provisions set out in the Agreement.		R

The table that follows immediately below identifies the Disaster Recovery Plan documents provided by Province and received by the Service Provider before the Hand-Over Date for which the Service Provider understands that Recovery Exercises have been conducted and that documented Recovery Exercise results will be made available to the Service Provider on the Hand-Over Date.

WTS Client	Application or Server	SP RTO Commitment	DR Plan
S15		<72 hours	S15

2.3.2 Acceptance of Disaster Recovery Plans Without Prior Recovery Exercise Results

From the second through to the end of the sixth month following the Hand-Over Date, the Service Provider and the Province will conduct a joint "Table-top Exercise" for all of those Disaster Recovery Plans that were provided by the Province to the Service Provider before the Hand-Over Date that lack Recovery Exercise results, as listed below in this Section 2.3.2 (*Acceptance of Disaster Recovery Plans Without Prior Recovery Exercise Results*). The Service Provider and Province shall jointly review these results in order to identify any gaps or issues relating to the effectiveness of the Service Provider's tasks set out in these Disaster Recovery Plans.

The following table lists the respective responsibilities of the Province and the Service Provider applicable to the acceptance of Disaster Recovery Plans without prior Recovery Exercise results.

Acceptance of Disaster Recovery Plans Without Prior Recovery Exercise Results	Responsibility	
	Province	Service Provider
From the second through to the end of the sixth month following the Hand-Over Date, conduct, jointly with the Province, a "Table-top Exercise" for all Disaster Recovery Plans which do not have associated Recovery Exercise results and review results with the Province.		R
From the second through to the end of the sixth month following the Hand-Over Date, conduct, jointly with the Service Provider, a "Table-top Exercise" for all Disaster Recovery Plans which do not have associated Recovery Exercise results and review results with the Service Provider.	R	
Provide to Service Provider written confirmation with respect to the results of the "Table-top Exercise", *i.e.*, whether the Disaster Recovery Plan objectives were validated to the satisfaction of the Province.	R	
Provide to Province written confirmation with respect to the results of the "Table-top Exercise", *i.e.*, whether the Disaster Recovery Plan objectives were validated to the satisfaction of Service Provider.		R
Update the Disaster Recovery Plan to incorporate issues and lessons learned as a result of the "Table-top Exercise".		R
If the "Table-top Exercise" results are not satisfactory to Province and Service Provider and additional assets or the services of a third party supplier are required, propose a change to the Disaster Recovery Plan. Such change is to be effected in accordance with the Governance Process or through the Change Order Process, as applicable, pursuant to the provisions set out in the Agreement.		R
Accept and add the Disaster Recovery Plan to the list of Service Provider Disaster Recovery Plans if the Disaster Recovery Plan has been effected in accordance with the Governance Process or through the Change Order Process as applicable pursuant to the provisions set out in the Agreement.		R
If the "Table-top Exercise" results are satisfactory to Province and Service Provider, accept the Disaster Recovery Plan and add the Disaster Recovery Plan to the list of approved Service Provider Disaster Recovery Plans.		R

Acceptance of Disaster Recovery Plans Without Prior Recovery Exercise Results	Responsibility	
	Province	Service Provider
Conduct the first annual Recovery Exercise within twelve (12) months of the Hand-Over Date, provided that resources to be provided by Province (as required by the Service Provider Disaster Recovery Plan) are available to Service Provider.		R
Act as liaison with the Province to coordinate and ensure that resources to be provided by the Province, as required by the Service Provider Disaster Recovery Plan, are communicated to the Province in writing so that the required resources can be made available to the Service Provider.		R

The table that follows immediately below identifies the Disaster Recovery Plan documents received from the Province for which Recovery Exercise results are not expected to be available. RTOs have been identified from the BCP documents identified in Section 2.1 (*Before Hand-Over Date*) above, or from the following Disaster Recovery Plan documents:

WTS Client	Application or Server	Client RTO Commitment	SP RTO Commitment	DR Plan

S15

2.3.3 Disaster Recovery Obligations that are not In-Scope for Acceptance by the Service Provider

The table that follows immediately below describes Disaster recovery commitments that were identified from the WTS BCPs for which the Service Provider has not received, before the Hand-Over Date, any Disaster Recovery Plans or the corresponding Recovery Exercise results.

Without documented Disaster Recovery Plans, the Service Provider cannot commit to achievement of the RTOs specified in the table below and will need to rely on its Commercially Reasonable Efforts described in Appendix C (*Service Provider Efforts*).

Accordingly, it will not be possible for the Service Provider to assume the Disaster recovery obligations corresponding to the RTOs for applications or servers identified in the following table.

WTS Client	Application or Server	Client RTO Commitment	SP RTO Commitment	DR Plan

S15

WTS Client	Application or Server	Client RTO Commitment	SP RTO Commitment	DR Plan

S15

In the event the subject Disaster Recovery Plan documents are not available and the Province or any Client, as applicable, wishes to obtain such plans, the Service Provider will upon request of the Province or such Client, as applicable, provide resources to draft the Service Provider Disaster Recovery Plans and carry out periodic Recovery Exercises that may be in addition to annual Recovery Exercises, all of the foregoing will be available on a Time and Materials basis. The Service Provider will propose fixed pricing for all required annual Recovery Exercises for any Disaster Recovery Plans developed upon request of the Province or any Client to be pre-paid by the Province at the time the completed plan is approved and accepted by the Province or Client.

2.3.4 Ongoing

During the term of the Agreement the Service Provider will update and maintain its initial BCP in respect of the Services. Additional obligations of the parties are in the table that follows.

Ongoing	Responsibility	
	Province	Service Provider
Maintain continuous service of a "Business Continuity Representative" and an alternate representative(s).		R
Maintain continuous service of a "Business Continuity Representative" and an alternate representative(s).	R	
Notify the Province and any Client, as applicable, in writing, within 3 Business Days of the relevant change, when the "Service Provider Business Continuity Representative" or alternate(s) change, or when contact information specifics change.		R
Notify the Service Provider, in writing, within 3 Business Days of the relevant change, when the "Customer Business Continuity Representative" or alternate(s) change, or when contact information specifics change.	R	
Participate in BCP and Disaster Recovery Plan integration with the Province as the Services are transformed.		R
Participate in BCP and Disaster Recovery Plan integration with the Service Provider as the Services are transformed.	R	
Implement and following implementation annually test and update Business Continuity Plan(s) and Disaster Recovery Plan(s) for continuity of the Service Provider internal service management systems.		R
Provide written confirmation to the Province annually that the Service Provider has conducted an annual test and update of the Business Continuity Plan(s) and Disaster Recovery Plan(s) for the continuity of Service Provider internal service management systems.		R
Conduct an annual BIA and SRA to validate that Service Provider's Business Continuity Plan(s) and Disaster Recovery Plan(s) are complete in the case of its internal service management systems.		R
Provide written confirmation to the Province annually that; the Service Provider has conducted an annual BIA and SRA and appropriately updated the Business Continuity Plan(s) and Disaster Recovery Plan(s) to reflect and address BIA findings to support the continuity of Service Provider internal service management systems.		R

Ongoing	Responsibility	
	Province	Service Provider
Conduct an annual BIA and SRA to validate that Service Provider BCP and Service Provider Disaster Recovery Plan(s) that support the Services are complete.		R
Provide written confirmation to the Province annually that the Service Provider has: conducted an annual BIA and SRA; and appropriately updated the Service Provider BCP and Service Provider Disaster Recovery Plan(s) to reflect and address BIA findings to support the Services.		R
Provide applicable Province Policy, standards and templates to the Service Provider that the Province requires the Service Provider to use, if any.	R	
Provide clarification or interpretation of the application of applicable Province Policy at the written request of the Service Provider.	R	
Manage the Service Provider's obligations in respect of business continuity and disaster recovery as set out in the Agreement.		R
Meet validated RTO necessary to successfully recover the Services.		R
Act as liaison with the Province to coordinate and ensure the integration of Service Provider BCP and Service Provider Disaster Recovery Plan(s) with those of the Province.		R
Participate in Business Continuity Plan and Disaster Recovery Plan integration with the Service Provider.	R	
Participate in Business Continuity Plan and Disaster Recovery Plan integration with the Province.		R
Maintain a complete list of approved Service Provider Disaster Recovery Plans which support the restoration and recovery of the Services, including dates of maintenance, approvals and exercise.		R
Provide a written summary report to the Province annually detailing the complete list of Service Provider Disaster Recovery Plans that support the Services, including dates of maintenance, approvals and exercise.		R
Perform annually, a review, Recovery Exercise and update of Business Continuity Plan(s) and Service Provider Disaster Recovery Plan(s) including consideration of Force Majeure Events and Labour Disruptions, all of which are in respect of the Services.		R

Ongoing	Responsibility	
	Province	Service Provider
Develop Recovery Exercises that include the coordination of multiple Disaster Recovery Plans that are activated simultaneously in order to validate their integration and coordinated response management in the event of a Disaster.		R
Develop a Province client guide or any Recovery Exercise related document references, except the Service Provider Disaster Recovery Plan(s), that may be required by the Province to effect the participation of the Province in a Recovery Exercise.	R	
Participate with the Province to develop a Province client guide or any Recovery Exercise related document references that may be required by the Province to effect the participation of the Province in a Recovery Exercise, especially where the reference information can only be provided or confirmed by the Service Provider.		R
Coordinate the Province participation in the Recovery Exercise, as may be necessary.	R	
Integrate and participate in the coordination of Province participation in the Recovery Exercise, as may be necessary.		R
Approve, as may be necessary, the scheduling of all Recovery Exercises.	R	
After each Recovery Exercise, conduct a customer satisfaction survey.		R
Participate in the customer survey conducted by the Service Provider after each Recovery Exercise.	R	
After each Recovery Exercise, complete and submit, within 30 days of the completion of the exercise, a report to the Province with respect to the scope, purpose, scenario, details, findings, issues, actions and outcomes of the Recovery Exercise, and an updated copy of the Service Provider Disaster Recovery Plan(s) for information purposes, with updates clearly marked.		R
Participate in the Service Provider's gathering of findings, issues actions and outcomes after each Recovery Exercise.	R	
Track the assignment, progress and completion of issues and actions after each Recovery Exercise.		R

Ongoing	Responsibility	
	Province	Service Provider
Provide to the Province a quarterly summary report of the assignment, progress and completion of issues and actions after each Recovery Exercise until all of the issues and actions of the Recovery Exercise have been deemed by the Province to be resolved or accepted.		R
Conduct an awareness and training program at the following times so that all relevant Service Provider Personnel, participants or responders in the Business Continuity Plan(s), the Service Provider Disaster Recovery Plan(s), and the Operations Centre Plan are familiar with their roles and responsibilities in order that an effective and coordinated response, recovery, resumption and/or continuance of service may be achieved: (a) for all Service Provider Personnel who are newly assigned to participate in the Services, or who are assigned roles in the Business Continuity Plan(s), Service Provider Disaster Recovery Plan(s) and/or Operations Centre Plan; (b) when Business Continuity Plan(s), Service Provider Disaster Recovery Plan(s), or the Operations Centre Plan are changed significantly; and (c) regularly, but not less than annually, to maintain the knowledge and skill levels of Service Provider Personnel and responders such that it will enable the Personnel or responders to effectively perform their roles if a BCP or Service Provider Disaster Recovery Plan is activated.		R
Provide a written summary report to the Province annually detailing the awareness and training events conducted by the Service Provider to support the program related to Business Continuity and Disaster Recovery Services supporting the Services.		R
Provide no less than ten Business Days written notice to the Service Provider for the Service Provider to submit any specified Business Continuity Plan (other than the BCP for the Data Centre Services in respect of which the Service Provider shall comply with the provisions of the Agreement) in order to demonstrate that the plan(s) complies with or otherwise conforms to applicable Province Policy.	R	

Ongoing	Responsibility	
	Province	Service Provider
Submit to the Province any BCP (other than the BCP for the Data Centre Services) specified in the written notice in order to demonstrate that the plan(s) comply with or otherwise conforms to applicable Province Policy.		R
Receive the specified Business Continuity Plan(s) for the Service Provider's Services (other than the BCP for the Data Centre Services) from time to time as deemed necessary by the Province to demonstrate that it complies with and otherwise conforms to applicable Province Policy.	R	
Upon receipt of written notice from the Province, or as otherwise identified by the Service Provider, update and amend the BCP to the extent required for the BCP to be fully compliant with the applicable Province Policy.		R
Develop, implement and maintain a Service Provider's Operations Centre Plan to include the details of declaration, plan activation and the coordinated response and response management resulting from a planned or unexpected disruption to Service causing the activation of Service Provider Disaster Recovery Plan(s). The plan shall include organizational structure, and detail all response roles and responsibilities, in keeping with, or integrating with, the British Columbia Emergency Response Management System (BCERMS), and shall establish and detail the communication links with the Province (such plan to be referred to herein as the "**Operations Centre Plan**").		R
Develop, implement and maintain a Province's Operations Centre Plan to include the details of declaration, plan activation and the coordinated response and response management resulting from a planned or unexpected disruption to Service causing the activation of Disaster Recovery Plan(s). The plan shall include organizational structure, and detail all response roles and responsibilities, in keeping with, or integrating with, BCERMS, and shall establish and detail the communication links with the Service Provider.	R	
Act as the liaison with the Province to coordinate and ensure the integration of the Service Provider's Operations Centre Plan into those of the Province, including notification and response contact information specifics.		R
Participate in Operations Centre Plan integration with the Service Provider.	R	

Ongoing	Responsibility	
	Province	Service Provider
Notify the Province and any Client, as applicable, in writing, within 3 Business Days of the relevant change, when the Service Provider Operations Centre Plan role assignments change or when contact information specifics change.		R
Notify the Service Provider, in writing, within 3 Business Days of the relevant change, when the Province's or Client's (as the case may be) Operations Centre Plan role assignments change or when contact information specifics change.	R	
Provide written confirmation to the Province annually that: the Service Provider has conducted an annual test and update of the Service Provider's Operations Centre Plan; and the updated plan has been reviewed and approved by senior Service Provider management.		R
Identify and inform the Province in writing of the need for Service Provider Disaster Recovery Plans in those situations wherein documented plans may not exist or in those cases wherein additional services are subscribed for or developed.		R
If the available recovery actions documented in the Service Provider's Business Continuity Plan(s) and Disaster Recovery Plan(s) are determined to be ineffective for the restoration of Services that are disrupted by a Force Majeure Event, then identify in the Service Provider Business Continuity Plan(s) that prudent and commercially reasonable efforts will be taken in cooperation with the Province and any Client, as applicable, in support of restoration of Services that are requested by the Province and such Client, as described in Appendix C (*Service Provider Efforts*).		R
Maintain a list of dedicated servers and dedicated storage, described in Section 3.3 (*Service Catalogue Offerings for Continuity of Services*) and 3.4 (*Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours*) of this SOW, and record the dates, details and status of all tests and validations.		R
Provide the Province annually a copy of the list of dedicated servers and dedicated storage, described in Section 3.3 (*Service Catalogue Offerings for Continuity of Services*) and 3.4 (*Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours*) of this SOW, which records the dates and status of all test and validations.		R

Ongoing	Responsibility	
	Province	Service Provider
Act as the liaison with the Province to coordinate and pre-plan the priority of restoration of applications and Services, in support of the Service Provider's efforts, detailed in Appendix C (*Service Provider Efforts*).		R
Act as the liaison with the Province to coordinate and pre-plan which non-production assets could be repurposed to facilitate restoration of services, in support of the Service Provider's efforts, detailed in Appendix C (*Service Provider Efforts*).		R
Participate with the Service Provider to pre-plan the priority of restoration of applications and Services, in support of the Service Provider's efforts detailed in Appendix C (*Service Provider Efforts*).	R	
Participate with the Service Provider to pre-plan which non-production assets could be repurposed to facilitate restoration of services, in support of the Service Provider's efforts detailed in Appendix C (*Service Provider Efforts*).	R	
Develop and maintain a priority list for restoration of applications and Services, in support of the Service Provider's efforts detailed in Appendix C (*Service Provider Efforts*).	R	
Develop and maintain a priority list for which non-production assets could be repurposed to facilitate restoration of services, in support of the Service Provider's efforts detailed in Appendix C (*Service Provider Efforts*).		R
Consult with the Service Provider's Operation Centre to determine or verify the priority for restoration of applications and Services, when the Service Provider has invoked prudent efforts in support of Appendix C (*Service Provider Efforts*).	R	
Consult with the Province's Operation Centre to determine or verify the priority for restoration of applications and Services, when the Service Provider has invoked prudent efforts, in support of Appendix C (*Service Provider Efforts*).		R
The Service Provider will maintain a monthly estimation of the available data centre resources (e.g., floor space and power) at its Canadian data centres and those of its DC Subcontractor to lessen the chance that in the event of a Disaster proper decisions and actions will be delayed, in support of Appendix C (*Service Provider Efforts*).		R
Provide a recommendation to the Province and request approval from the Province to shut down some non-critical virtual guest servers, in support of Appendix C (*Service Provider Efforts*).		R

Ongoing	Responsibility	
	Province	Service Provider
Approve in its sole discretion some non-critical virtual guest servers to be shut down after considering the recommendation and request from the Service Provider, in support of Appendix C (*Service Provider Efforts*).	R	

In the event of a Disaster affecting the Province's systems or applications for which there is no effective Disaster Recovery Plan, the Service Provider will use prudent efforts, including Service Provider Efforts, to restore service, as described in Appendix C (*Service Provider Efforts*).

3. CONTINUITY ENABLERS IN THE SOLUTION

This section describes services that will be available for developing new or enhanced business continuity treatments and provides specific examples of how they could be applied to create or enhance Disaster Recovery Plans for WTS services or WTS hosted Client Ministry applications that may require more robust business continuity and Disaster recovery treatments than are afforded by the Business Continuity Plans and Disaster Recovery Plans assumed as set out in Section 2 (*Assumption by Service Provider of Responsibility for Managing the Continuity of the Services*) of this Statement of Work.

3.1 Business Continuity Plan and Disaster Recovery Plan Development

The Service Provider offers, additionally to the Province and any Client, any or all specific components of BCP development, maintenance and exercise, for business of the Province. A sample Statement of Work for such additional services may be found in Appendix E (*Sample SOW for Disaster Recovery Plan Development*).

Service Provider Disaster Recovery Plan development will be provided by the Service Provider for the development of new Service Provider Disaster Recovery Plans in support of additional or new services. A sample Statement of Work for such additional services may be found in Appendix E (*Sample SOW for Disaster Recovery Plan Development*).

The Service Provider offers, additionally to the Province and any Client, any or all specific components of Disaster Recovery Plan development, maintenance and Recovery Exercise, for business applications and services that are supported by the Services. A sample Statement of Work for such additional services may be found in Appendix E (*Sample SOW for Disaster Recovery Plan Development*).

Additional BCP and Disaster Recovery Plan Development Services	Responsibility	
	Province	Service Provider

Additional BCP and Disaster Recovery Plan Development Services	Responsibility	
	Province	Service Provider
Provide Disaster Recovery Plan development services on a Time and Materials basis for the development of Service Provider Disaster Recovery Plans for those Services included in Section 2.3.3 (*Disaster Recovery Obligations that are not In-Scope for Acceptance by the Service Provider*).		R
Accept the completed Service Provider Disaster Recovery Plan(s) developed for those Services included in Section 2.3.3 (*Disaster Recovery Obligations that are not In-Scope for Acceptance by the Service Provider*), and add them to the list of approved Service Provider Disaster Recovery Plans.		R
Provide Service Provider Disaster Recovery Plan development services on a Time and Materials basis for the development of new Service Provider Disaster Recovery Plans in support of additional or new services excluding those Disaster Recovery Plans identified and assumed as set out in Section 2.3.1 (*Acceptance of Previously Exercised Plans*) or 2.3.2 (*Acceptance of Disaster Recovery Plans Without Prior Recovery Exercise Results*) of this Statements of Work, or where Service Provider Disaster Recovery Plans have been added to the approved Service Provider Disaster Recovery Plan list.	C	R
Provide quotes for all required annual Recovery Exercises for any new Service Provider Disaster Recovery Plans developed by the Service Provider.		R
Accept and add completed Service Provider Disaster Recovery Plan(s), developed for additional or new services, to the list of approved Service Provider Disaster Recovery Plans.		R
Offer additional Disaster Recovery Plan development services on a Time and Materials basis for the development of Disaster Recovery Plans for the Province's internal business applications and services that are supported by the Services.	C	R
Offer additional BCP development services on a Time and Materials basis for the development of BCPs for the Province's internal business.	C	R
Offer additional Recovery Exercise(s) on a Time and Materials basis only where the Province requests Recovery Exercises of a specific Service Provider Disaster Recovery Plan that exceeds the annual required exercise for that plan.	C	R

Additional BCP and Disaster Recovery Plan Development Services	Responsibility	
	Province	Service Provider
Offer additional "Table-top Exercise(s)" on a Time and Materials basis only where the Province requests "Table-top Exercise" of a specific Service Provider Disaster Recovery Plan that exceeds the annual required exercise for that plan, excluding the "Table-top Exercise" described in Section 2.3.2 (*Acceptance of Disaster Recovery Plans Without Prior Recovery Exercise Results*) of this Statement of Work.	C	R

3.2 Service Catalogue Offerings for Continuity of Services

Service Provider's Services Catalogue offerings for continuity of Services are the basic building block concepts that can be used to provide continuity services in the event of a Disaster. This Section 3.2 presents sample scenarios based on RTO and specific deliverables of such services.

(a) To achieve RTO between 24 and 72 hours, Service Provider requires the use of backup services and designated capacity (servers, storage, network access, and power) at an alternate data centre that is either reserved or re-purposed from another use, such as systems development or application/system testing.

(b) To achieve RTO between 4 and 24 hours, the Service Provider requires the use of backup services and reserved spare capacity (servers, storage, network access, and power) at the alternate data centre that is immediately ready to use.

(c) To achieve RTO in the range of 10 minutes to 4 hours, the Service Provider recommends the use of the Service Catalogue offering known as "Tier 1 – Business Priority – Geographically Distributed Cluster (with asynchronous data replication)", SKUs WAP-001*, WIN-001, WDV-001, or WCS-001.

(d) To provide *ad hoc* reports, documentation or submissions that are in addition to those required within the Statement of Work, the Service Provider offers Professional Services on a Time and Materials basis.

(e) To provide "Table-top Exercise" or Recovery Exercise that exceeds the annual requirement for Service Provider Disaster Recovery Plan(s) within the Statement of Work, the Service Provider offers Professional Services on a Time and Materials basis.

3.3 Service Catalogue Disaster Recovery Reserve Units

Service Provider offers Windows Tier 1, 2 and 3 Virtual Image reserve units (SKU VWLH-001/002/003). These reserve units are available by selecting the appropriate tier Virtual Images and the power from the Services Catalogue. These reserve units will be located in the recovery data center and will not be used for normal processing. Once 20 Windows Virtual Image reserve

units have been ordered, a dedicated server will be selected and placed in a standby mode outside of the online capacity. This server will be operationally tested monthly to validate readiness and will only be used for Disaster Recovery Exercises and in the event of an actual Disaster.

Service Provider offers Solaris Tier 1, 2 and 3 Virtual Image reserve units (SKU VSH-001/002/003). These reserve units are available by selecting the appropriate tier Virtual Images and the power from the Services Catalogue. These reserve units will be located in the recovery data centre and will not be used for normal processing. Once 20 Solaris Virtual Image reserve units have been ordered, a dedicated server will be selected and placed in a standby mode outside of the online capacity. This server will be operationally tested monthly to validate readiness and will only be used for Disaster Recovery Exercises and in the event of an actual Disaster.

Service Provider offers AIX WPAR Tier 1, 2 and 3 Virtual Image reserve units (SKU VAH-001/002/003). These reserve units are available by selecting the appropriate tier Virtual Images and the power from the Service Catalogue. These reserve units will be located in the recovery data centre and will not be used for active workload processing. Once 20 AIX WPAR Virtual Image reserve units have been ordered, a dedicated server will be selected and placed in a standby mode. This server will be operationally tested monthly to validate readiness and will only be used for a Disaster Recovery Exercises and in the event of an actual Disaster.

Service Provider offers Tier 1 and 2 Storage reserve units (in Gigabytes). These reserve units are available by selecting the appropriate tier Storage Reserve, by the Gigabyte, from the Services Catalogue. These dedicated reserves will be located in the recovery data centre and will not be used for active storage operations. This dedicated Storage will be validated monthly and will be used for a Recovery Exercise and in the event of an actual Disaster.

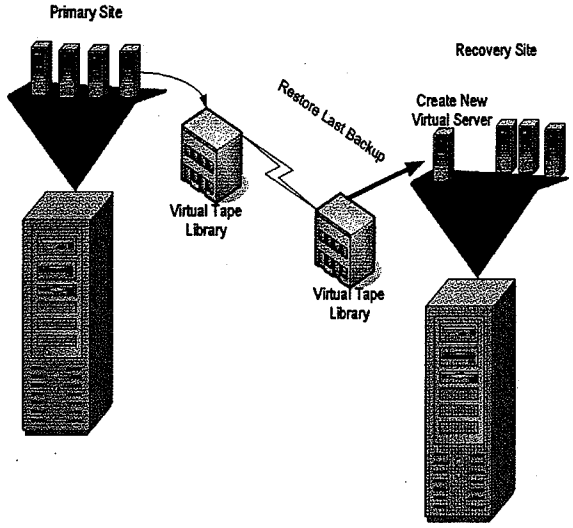
3.4 Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours

Disaster Recovery Scenarios to Achieve RTO between 24 and 72 Hours consists of developing and maintaining a plan for recovering the server operating system on an equivalent system platform(s) so that application recovery can be performed by the Province or any Client or its service provider. This recovery is typically accomplished via restore from a backup tape or virtual tape to the targeted system(s). The Service Provider will support the hosting of Province supplied infrastructure dedicated or re-purposed to providing Disaster recovery.

Server hardware reserve components that are selected will normally be powered down and out of service; however, a monthly power-up test and validation will be conducted. The hardware will only be used in the event of a scheduled Disaster Recovery Exercise or an actual Disaster.

The following scenarios will support RTO between 24 and 72 hours.

Windows DR Building Blocks - Virtual Server

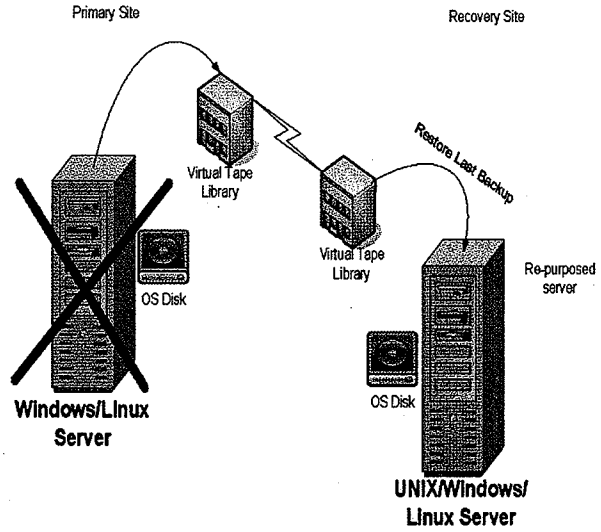


(i) Select Tier 1, 2 or 3 Virtual Image (primary site) from the Services Catalogue.
(ii) Select Tier 1, 2 or 3 Storage from the Services Catalogue.
(iii) Select Core Backup from the Services Catalogue.
(iv) Select Disaster Recovery Plan/Test from the Services Catalogue.
(v) Select Virtual Image Reserve (alternate site) from the Services Catalogue. *
(vi) Select Storage Reserve (alternate site) from the Services Catalogue. *

*Alternately, re-purpose assets from designated non-essential servers.

Reserve: For each 20 Tier 1, 2 or 3 Virtual Image reserve selected, Service Provider will dedicate one host server for Disaster recovery, as outlined in Section 3.3 (*Service Catalogue Disaster Recovery Reserve Units*). All Storage Reserves will be dedicated at time of order.

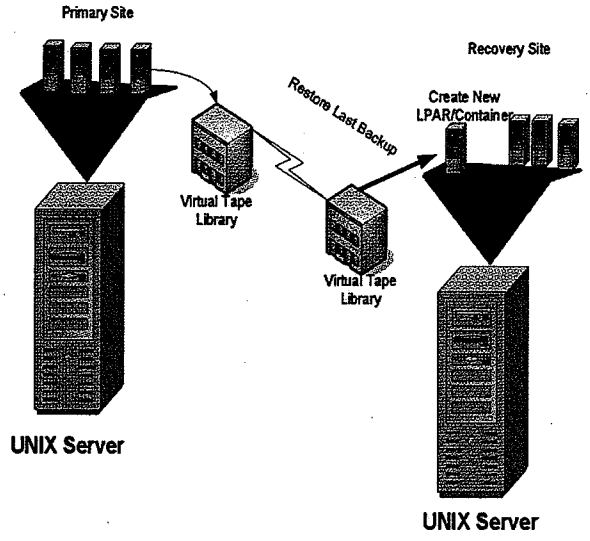
Wintel DR Building Blocks - Physical Server



(i) Select Tier 1, 2 or 3 Server (primary site) from the Services Catalogue.
(ii) Select Tier 1, 2 or 3 Storage from the Services Catalogue.
(iii) Select Core Backup from the Services Catalogue.
(iv) Select Disaster Recovery Plan/Test from the Services Catalogue.
(v) Select Tier 1, 2 or 3 Server (alternate site) from the Services Catalogue. *
(vi) Select Storage Reserve (alternate site) from the Services Catalogue. *

* Alternately, re-purpose assets from other designated non-essential services.

UNIX DR Building Blocks - Container/WPAR



(i) Select Tier 1, 2 or 3 Container or WPAR Image (primary site) from the Services Catalogue.

(ii) Select Tier 1, 2 or 3 Storage from the Services Catalogue.

(iii) Select Core Backup from the Services Catalogue.

(iv) Select DR Recovery Plan/Test from the Services Catalogue.

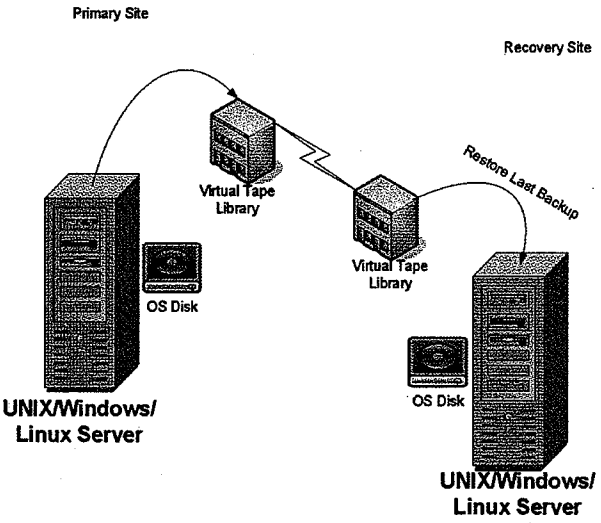
(v) Select Container or WPAR Image Reserve (alternate site) from the Services Catalogue. *

(vi) Select Storage Reserve (alternate site) from the Services Catalogue. *

*Alternately, re-purpose assets from other designated non-essential services.

Reserve: For each 20 Tier 1, 2 or 3 Container or WPAR Image reserve selected, Service Provider will dedicate one host server for Disaster recovery, as outlined in Section 3.3 (*Service Catalogue Disaster Recovery Reserve Units*). All Storage Reserves will be dedicated at time of order.

Unix or Linux DR Building Blocks - Physical Server



(i) Select Tier 1, 2 or 3 Server (primary site) from the Services Catalogue,

(ii) Select Tier 1, 2 or 3 Storage from the Services Catalogue,

(iii) Select Core Backup from the Services Catalogue,

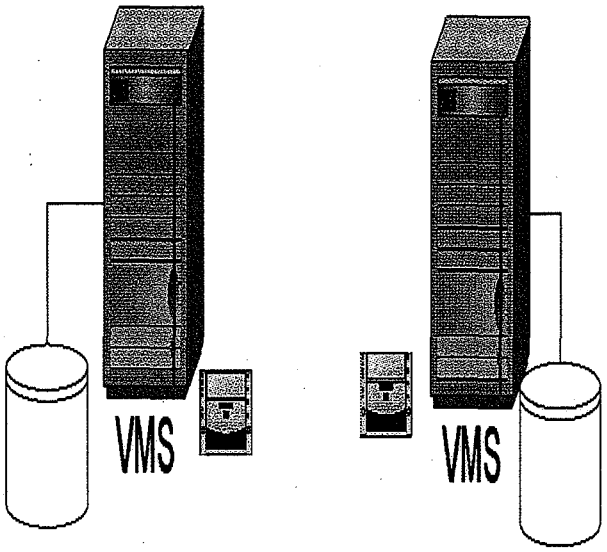
(iv) Select DR Recovery Plan/Test from the Services Catalogue,

(v) Select Tier 1, 2 or 3 Server (alternate site) from the Services Catalogue, *

(vi) Select Storage Reserve (alternate site) from the Services Catalogue, *

*Alternately, re-purpose assets from other designated non-essential services.

VMS Systems DR – Physical Server



Assumptions

(i) Disaster Recovery Plan for VMS systems currently in place will be maintained until an STMS Data Centre becomes available.

(ii) Staff and tapes move physically to recovery site.

(iii) When an STMS Data Centre becomes available:

(a) Existing Province servers that are held in reserve for VMS System (the "Recovery Server") will be moved into an STMS Data Centre, racked and cabled when data centres become available.

(b) Updated Disaster Recovery Plans will be prepared.

(c) Recovery Exercise is intended shortly after migration.

The following table lists responsibilities with respect to Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours.

Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours	Responsibility	
	Province	Service Provider
Initiate a prompt declaration of Disaster if the primary data centre is rendered unusable and notify the Province in accordance with the applicable Business Continuity and Disaster Recovery Plans.		R
Notify Province, in writing, of declaration and activation of the relevant Disaster Recovery Plan(s).		R
Activate the Service Provider Operations Centre Plan and Service Provider Disaster Recovery Plan(s).		R
Activate the Province's Operations Centre Plan.	R	

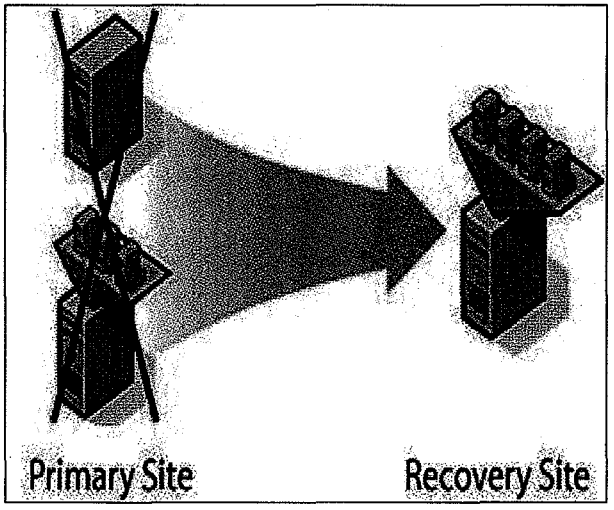
Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours	Responsibility	
	Province	Service Provider
Facilitate secure access to recovery hardware at an alternate location during Recovery Exercises and when a Disaster occurs.		R
Support Service Provider secure access to recovery hardware at an alternate location during Recovery Exercises and when a Disaster occurs.	R	
Provide Personnel and prearrange material and resources to achieve RTO for designated systems and Service Provider Disaster Recovery Plans.		R
Coordinate with Province and schedule annual Recovery Exercises in a manner that is functionally and operationally progressive in terms of varying the Disaster scenarios and varying combinations of different recovery strategies (such as availability of key personnel) to increase complexity and improve expected results.		R
Coordinate with Service Provider and schedule annual Recovery Exercises in a manner that is functionally and operationally progressive in terms of varying the Disaster scenarios and varying combinations of different recovery strategies (such as availability of key personnel) to increase complexity and improve expected results.	R	
Perform the following: (i) One Recovery Exercise annually of the hardware platform and operating system (Service Provider Disaster Recovery Plan). (ii) Record issues and lessons learned. (iii) Draft Executive Summary. (iv) Assign and track action items. (v) Service Provider Disaster Recovery Plan updates. (vi) Maintain Service Provider Disaster Recovery Plan. (vii) Draft other administrative documentation to improve the then existing Disaster Recovery Plan.		R

Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours	Responsibility	
	Province	Service Provider
In the case of Service Provider Disaster Recovery Plans accepted by the Service Provider, the Service Provider will provide system support to the Province or the Province's application(s) provider for one annual concurrent Recovery Exercise of the application(s), data and server.		R
Provide Service Provider with a written list of Province's third party suppliers that will be required to develop Disaster Recovery Plans and participate in a "Table-top Exercise", a Recovery Exercise or an actual Disaster.	R	
Confirm with Province's third party suppliers that their recovery responsibilities are understood and their plans are consistent with the expectations for RTOs.	R	
Confirm that the Province's third party suppliers have performed the recovery of the application(s) and data during the scheduled annual Recovery Exercise and at the time of an actual Disaster.	R	
Maintain financial responsibility in respect of Province's third party suppliers in the case of agreements for Disaster Recovery Services, their Disaster Recovery Plan exercises, and implementation of their Disaster Recovery Plans.	R	
Maintain financial responsibility for Disaster recovery resources including, servers and storage, data centre power, network access.	R	
Securely pack, ship, stage, and return media, such as tapes, including reconciliation and tracking compliant with GCIO Information Security, at the recovery site for annual Recovery Exercises and at time of an actual Disaster.		R
Maintain financial responsibility for all travel expenses including, but not limited to, air fare, hotel accommodation, food, and rental car incurred by Service Provider personnel and its agents where travel is required to perform a "Table-top Exercise", Recovery Exercise or at the occasion of an actual Disaster.		R
Maintain financial responsibility for all travel expenses including, but not limited to, air fare, hotel accommodation, food, and rental car incurred by Province personnel and its agents where travel is required to perform a "Table-top Exercise", Recovery Exercise or at the occasion of an actual Disaster.	R	

3.5 Disaster Recovery Measures to Achieve RTO between 4 and 24 Hours

Disaster Recovery Scenarios to Achieve RTO between 4 and 24 Hours consists of developing and maintaining a plan for recovering the server operating system on an equivalent system platform(s) so that application recovery can be performed by the Client or by the Client's application(s) provider. This recovery is typically done via backup tape or virtual tape to targeted systems.

Server hardware reserve components that are selected will normally be powered down and out of service; however, a monthly power-up test will be conducted to validate readiness. The hardware will only be used in the event of a scheduled Recovery Exercise or an actual Disaster.



Resources for Disaster recovery must be dedicated to Disaster recovery purposes. Hardware is selected from the Services Catalogue for the server(s). All storage for the servers must be on replicated storage. This storage can be selected in the Services Catalogue for the storage in question by ensuring that Client has selected Tier 1, DR Copy @ Alternative Site w/ DR Clone (Mirrored Primary) Or Tier 1, DR Copy @ Alternative Site w/ DR Clone (Standard). Alternatively data can be replicated by customer supplied software/hardware between running systems.

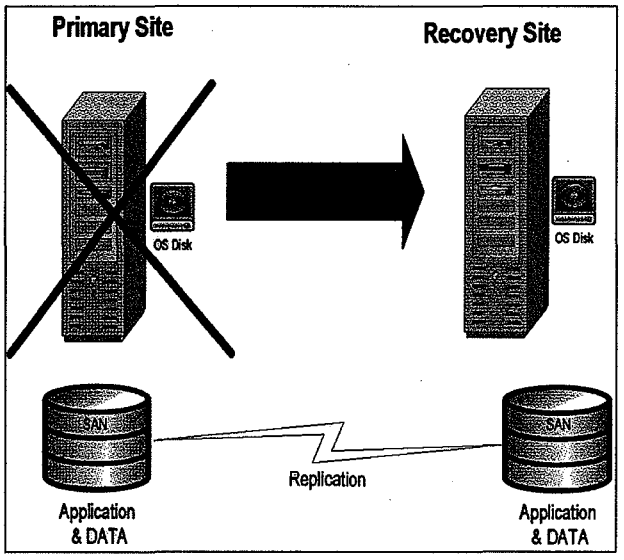
The following scenarios will support RTO between 4 and 24 hours.

Wintel DR Building Blocks - Virtual Image

(i) Select Tier 1, 2 or 3 Virtual Image (primary site) from the Services Catalogue
(ii) Select Tier 1, DR Copy @ Alternative Site w/ DR Clone (Standard) Storage from the Services Catalogue
(iii) Select Core Backup from the Services Catalogue
(iv) Select DR Recovery Plan/Test from the Services Catalogue
(v) Select Tier 1, 2 or 3 Virtual Image Reserve (alternate site) from the Services Catalogue

Reserve: For each 20 Tier 1, 2 or 3 Virtual Image reserve selected, Service Provider will dedicate one host server for Disaster recovery.

Wintel DR Building Blocks - Physical Server



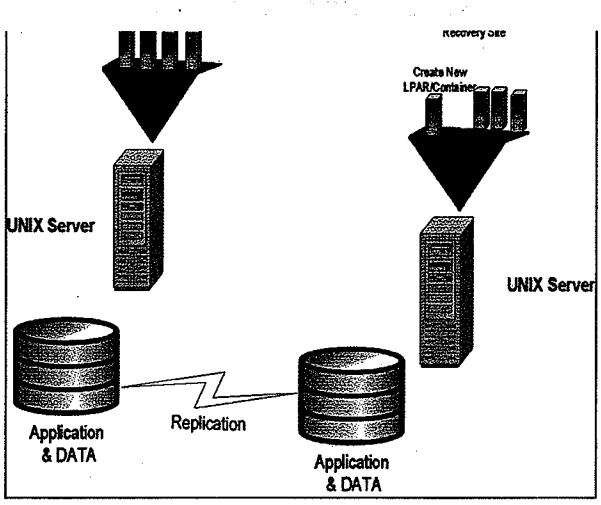
(i) Select Tier 1, 2 or 3 Virtual Image (primary site) from the Services Catalogue

(ii) Select Tier 1, DR Copy @ Alternative Site w/ DR Clone (Standard) Storage from the Services Catalogue

(iii) Select Core Backup from the Services Catalogue

(iv) Select DR Recovery Plan/Test from the Services Catalogue

(v) Select Tier 1, 2 or 3 Virtual Image Reserve (alternate site) from the Services Catalogue



UNIX DR Building Blocks - Container or WPAR

(i) Select Tier 1, 2 or 3 Container or WPAR Image (primary site) from the Services Catalogue

(ii) Select Tier 1, DR Copy @ Alternative Site w/ DR Clone (Standard) Storage from the Services Catalogue

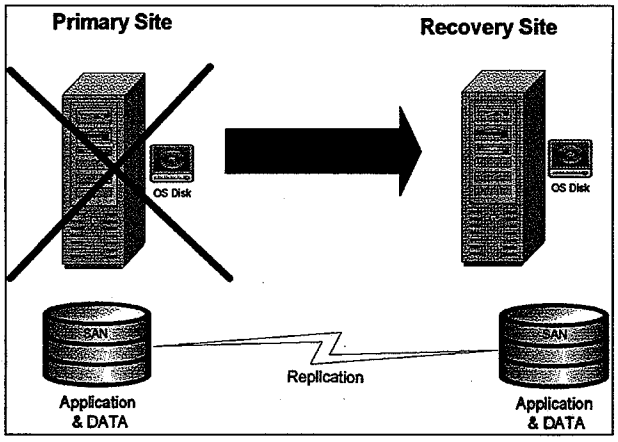
(iii) Select Core Backup from the Services Catalogue

(iv) Select DR Recovery Plan/Test from the Services Catalogue

(v) Select Container or WPAR Image Reserve (alternate site) from the Services Catalogue

Reserve: For each 20 Tier 1, 2 or 3 Container or WPAR Image reserve selected, Service Provider will dedicate one host server for Disaster recovery.

Unix or Linux DR Building Blocks - Physical Server



(i) Select Tier 1, 2 or 3 Server (primary site) from the Services Catalogue

(ii) Select Tier 1, DR Copy @ Alternative Site w/ DR Clone (Standard) Storage from the Services Catalogue

(iii) Select Core Backup from the Services Catalogue

(iv) Select DR Recovery Plan/Test from the Services Catalogue

(v) Select a Tier 1, 2 & 3 Server Reserve (alternate site) from the Services Catalogue

Responsibilities

The following table lists the respective responsibilities of the Province and the Service Provider with respect to Disaster Recovery Measures to Achieve RTO between 4 and 24 Hours.

Disaster Recovery Measures to Achieve RTO between 4 and 24 Hours	Responsibility	
	Province	Service Provider
Initiate a prompt declaration of Disaster if the primary data centre is rendered unusable and notify the Province in accordance with the applicable Business Continuity and Disaster Recovery Plans.		R
Notify Province, in writing, of declaration and activation of the relevant Disaster Recovery Plan(s).		R
Activate the Service Provider Operations Centre Plan and Service Provider Disaster Recovery Plan(s).		R
Activate the Province's Operations Centre Plan.	R	
Facilitate secure access to recovery hardware at an alternate location during Recovery Exercises and when a Disaster occurs.		R
Support Service Provider secure access to recovery hardware at an alternate location during Recovery Exercises and when a Disaster occurs.	R	
Provide Personnel and prearrange material and resources to achieve RTO for designated systems and Service Provider Disaster Recovery Plan(s).		R
Coordinate with Province and schedule annual Recovery Exercises in a manner that is functionally and operationally progressive in terms of varying the Disaster scenarios and varying combinations of different recovery strategies (such as availability of key personnel) to increase complexity and improve expected results.		R
Coordinate with Service Provider and schedule annual Recovery Exercises in a manner that is functionally and operationally progressive in terms of varying the Disaster scenarios and varying combinations of different recovery strategies (such as availability of key personnel) to increase complexity and improve expected results.	R	

Disaster Recovery Measures to Achieve RTO between 4 and 24 Hours	Responsibility	
	Province	Service Provider
Perform the following: (i) One Recovery Exercise annually of the hardware platform and operating system (Disaster Recovery Plan). (ii) Record issues and lessons learned. (iii) Draft Executive Summary. (iv) Assign and track action items. (v) Update the Service Provider Disaster Recovery Plan. (vi) Maintain the Service Provider Disaster Recovery Plan. (vii) Draft other administrative documentation to improve the then existing Disaster Recovery Plan.		R
In the case of Service Provider Disaster Recovery Plans, the Service Provider will provide system support to the Province or the Province's application(s) provider for one annual concurrent Recovery Exercise of the application(s), data and server.		R
Provide Service Provider with a written list of Province's third party suppliers that will be required to develop Disaster Recovery Plans and participate in a "Table-top Exercise", a Recovery Exercise or an actual Disaster.	R	
Confirm with Province's third party suppliers that their recovery responsibilities are understood and their plans are consistent with the expectations for RTOs.	R	
Confirm that the Province's third party suppliers have performed the recovery of the application(s) and data during the scheduled annual Recovery Exercise and at the time of an actual Disaster.	R	
Maintain financial responsibility in respect of Province's third party suppliers in the case of agreements for Disaster Recovery Services, their Disaster Recovery Plan exercises, and implementation of their Disaster Recovery Plans.	R	
Maintain financial responsibility for Disaster recovery resources including, servers and storage, data centre power, network access.	R	

Disaster Recovery Measures to Achieve RTO between 4 and 24 Hours	Responsibility	
	Province	Service Provider
Securely pack, ship, stage, and return media, such as tapes, including reconciliation and tracking compliant with GCIO Information Security, at the recovery site for annual Recovery Exercises and at time of an actual Disaster.		R
Maintain financial responsibility for all travel expenses including but not limited to air fare, hotel accommodation, food, and rental car incurred by the Service Provider Personnel and its agents where travel is required to perform a "Table-top Exercise", Recovery Exercise or on the occasion of an actual Disaster.		R
Maintain financial responsibility for all travel expenses including but not limited to air fare, hotel accommodation, food, and rental car incurred by Province personnel and its agents where travel is required to perform a "Table-top Exercise", Recovery Exercise or on the occasion of an actual Disaster.	R	

3.6 Geographically Dispersed Cluster Offerings With Very High Service Level Commitments for Applications that Require RTO of Less Than 4 Hours

To achieve an RTO in the range of ten minutes to four hours, the Service Provider recommends the use of the service catalogue offering known as "Tier 1 – Business Priority – Geographically Distributed Cluster (with asynchronous data replication)".

4. FUTURE BUSINESS CONTINUITY AND DISASTER RECOVERY OPPORTUNITIES

As the scale of Business Continuity and Disaster Recovery Services grows, there may be additional cost effective Business Continuity and Disaster recovery technologies available as a result of leveraging the larger scale of such services. The Service Provider, through leadership, will bring new opportunities to the Province that might be available in the future through technological advancement such as improved Virtual Server capabilities, improved storage capabilities, and high availability clustering advancements. This Section includes some examples that may be addressed as potential future service transformation opportunities (refer to the Transformation SOW relating to the Services).

Shared mainframe recovery between S15

- Each organization to rely on the other for emergency backup capacity and eliminate third party provider expense associated with Disaster Recovery Plans.

Managed Disaster Recovery Services

- A complete service offering for co-location Clients.

Disaster Recovery Test Services

- Planning and execution of Disaster Recovery Exercises in support of a Province's BCP.
- Executive summary outcome reports.
- Could be limited to hardware and OS or could include application recovery.

Offsite vaulting (electronic)

S15 eeking a solution that would be near the backup site.

Exchange recovery solutions

- Shared Disaster Recovery Plan capacity for Exchange services of multiple Clients.

Test / Dev Servers

- Pooling the test/development resources from multiple Clients as a shared capacity reserve for use in Disaster Recovery Plans.

Appendix A –Definitions

This Appendix includes a list of terms used within this Statement of Work including the Appendices attached to and incorporated therein.

Definable Term	Definition
"Agreement"	Master Services Agreement dated March 30, 2009 between Her Majesty the Queen in right of the Province of British Columbia and EDS Advanced Solutions Inc.
"Applications"	Means any software developed or licensed by the Province (including, for greater certainty, Clients) that provides functions that are required by a Client in support of its business processes
"BCP"	Business Continuity Plan, as such term is defined in the Agreement
"Business Continuity and Disaster Recovery Services"	The services described in Section 1.3 of this SOW.
"Business Continuity Services"	The services described in Article 17 (*Business Continuity*) of the Agreement.
"Business Impact Assessment" or "BIA"	The Business Impact Analysis determines the effect that each type of potential threat, identified in a risk assessment, has on various functions or departments within an organization.
"Container"	A Sun Microsystems technology that allows for multiple instances of functionally independent operating systems and application on a single computer systems.
"Continuity Enablers"	Modular services and technologies that the Service Provider has developed to offer Disaster Recovery Services to the Province.
"DC Subcontractor"	Has the meaning set out in Schedule 5 (Special Terms) of the Agreement.
"Disaster Recovery Exercise"	A process by which a group of people follow a Disaster Recovery Plan step by step to its conclusion to validate all components of the pre-defined recovery plan in full-scale simulation to ensure that the Disaster Recovery Plan will achieve the business objectives as stated in the Disaster Recovery Plan.
"Disaster Recovery Plan (DRP)"	The plan which documents and describes the process, steps and actions that will be taken to recover and restore availability of IT systems in the event of a disruption, loss or Disaster.
"Disaster Recovery Planning"	Has the meaning given to it in Section 1.1 of Appendix D of this SOW.

Definable Term	Definition
"Disaster Recovery Measures to Achieve RTO between 24 and 72 Hours"	Means the services described in Section 3.4 of this SOW.
"Disaster Recovery Measures to Achieve RTO between 4 and 24 Hours"	Means the services described in Section 3.5 of this SOW.
"Disaster Recovery Services"	Services for developing and rehearsing advance arrangements and procedures that enable an organization to respond to a Disaster and resume critical business functions within a predetermined period of time, minimize the amount of loss and repair or replace damaged assets or facilities as soon as possible.
"Disaster Recovery Site"	Has the meaning given to it in the introductory paragraph of Appendix D of this SOW.
"Disaster Recovery Test"	Has the meaning given to it in Section 1.2 of Appendix D of this SOW.
"GCIO"	Government Chief Information Officer.
"GCIO Information Security"	The policies and procedures that the GCIO mandates that the Province and the Province's agents adhere to.
	S15
"IT Recovery Exercise (ITRE)"	An annual activity that exercises the Disaster Recovery Plan for the Managed Mainframe Services delivered by the Service Provider. The exercise includes the recovery of the System and a subset of Client Applications.
"Labour Disruption Plan"	A written plan describing the actions to take in the event of a Labour Disruption.
"Mainframe System"	Has the meaning given to it in the Managed Mainframe Services SOW.
"Mainframe System Software"	Has the meaning given to it in the Managed Mainframe Services SOW.
"Managed Mainframe Services"	Has the meaning given to it in the Managed Mainframe Services SOW.
"Operations Centre Plan"	Has the meaning given to it in Section 2.3.4 of this SOW.
"OS"	A hardware platform Operating System.
"Personnel"	Employees and independent contractors of the Service Provider.

Definable Term	Definition
"Recovery Centre"	The other data centre not housing the production workload to be recovered due to a Disaster.
"Recovery Exercise"	Same as "Disaster Recovery Exercise".
"Recovery Server"	Has the meaning given to it in Section 3.4 of this SOW.
"Satisfaction Survey"	A printed form or web based interview used to collect input from participants and stakeholders after the completion of a Disaster Recovery Exercise. Each survey is designed based upon the Disaster Recovery Exercise scenario that is used.
"Service Provider Efforts"	Refer to Appendix C attached to this Statement of Work.
"Storage Reserve"	Storage purchase from the Service Catalogue to be held as reserve capacity in support of the requirements of Disaster Recovery Plan.
"Strategic Risk Assessment" or "SRA"	A Strategic Risk Assessment is a formal process of identifying and evaluating risks that pose threats to the on-going success and operation of the business.
"Table-top Exercise"	A desktop process walkthrough of a Disaster Recovery Plan designed to evaluate the logic and content of the plan.
"WPAR"	An IBM technology that allows for multiple instances of functionally independent operating systems and application on single computer systems.
"Virtual Image"	A Virtual Server purchased from the Service Catalogue to be held as reserve capacity in support of the requirements of a Disaster Recovery Plan.
"Virtual Server"	An instance of a functionally independent operating systems and application on single computer systems.

Appendix B - Reports

Executive Summary Report

(Recovery Exercise) Executive Summary Report to be developed in keeping with established format, contents and detail of existing WTS Executive Reports completed for the annual IT Recovery Exercise.

Satisfaction Survey

(Recovery Exercise) Satisfaction survey to be developed in keeping with established format, contents and detail of existing customer satisfaction survey completed for the annual IT Recovery Exercise.

In the event a Disaster is declared, Service Provider's support services includes provision for invocation of relevant BCPs which in turn will may result in invocation of applicable Disaster Recovery Plans for the recovery and restoration of Service Provider Services. Furthermore, the Service Provider is responsible for specific tasks in Business Continuity or Disaster Recovery Plans which may be supported by the Services.

In addition to executing applicable Service Provider BCP and Service Provider Disaster Recovery Plans, Service Provider will use prudent and commercially reasonable efforts to recover and restore services that are not covered by these plans, or where the plans are determined to be ineffective to recover and restore the Services. For this purpose, Service Provider assumes that Service Provider and the Province would pre-plan the priority of restoration of applications and services and they would also pre-plan which non-production assets could be repurposed to facilitate restoration of services. The pre-planned priorities can be changed at the time of a Disaster, if appropriate.

In the event there is insufficient reserve capacity for recovery of all services the response will include the use of prudent and commercially reasonable efforts to find suitable alternative facilities, engaging suppliers to manufacture replacement equipment, engaging carriers to provide required network connectivity, reassignment and use of Service Provider staff who are not normally dedicated to the provision of Services to meet the objectives of Service Provider Efforts.

1. DISASTER RECOVERY MEASURES

In respect of general Disaster recovery measures, "Service Provider Efforts" will include without limitation the following:

1.1 Identify Service Provider, DC Subcontractor or Third Party Canadian Data Centre Capacity

In the case when a data centre becomes inaccessible during a Disaster, and Services are no longer available at that site, Service Provider will promptly attempt to procure capacity at a facility to house equipment to be used to recover and restore the Services. The Service Provider will consider its own facilities and those of other providers, in order of geographic preference, of British Columbia, Canada, and, then, the United States or other countries with permission of the Province. Acquiring the necessary facility and capacity will depend on what is available at fair market value unless the Province elects to cover incremental costs for space available facility and capacity at a premium to fair market value.

1.2 Leverage Available Service Provider Resources to Support Recovery

Service Provider has an extensive internal wide area network and a skilled workforce located throughout Canada. Service Provider will quickly engage skilled resources to support critical recovery operations if alternate workforce is needed as a result of the Disaster.

1.3 Leverage Relationships with Carriers to Acquire Required Network Circuits from SPAN/BC and Service Provider to Alternate Sites.

Service Provider and the Province have designed their networks to be as resilient as feasible to eliminate impact of Disasters. In the event of failure of the Services or a move to an alternate data centre facility, Service Provider will engage telecom carriers to provision necessary circuits. These circuits may be from a Service Provider facility to a recovery site or from a recovery site to the SPAN/BC network.

1.4 Support Acquisition of Replacement Equipment for Both Server and Storage Infrastructures.

In the event of a Disaster, it may be necessary to replace equipment to facilitate recovery and restoration. Service Provider will enter into supply arrangements to have new equipment ready to ship within 10 Business Days of submission of its request, for most types of Service Provider equipment. Tier 1 storage equipment is expected to be supplied or ready to ship within 30 Business Days or a shorter period, if the Disaster is of a localized nature, affecting a single facility and not an entire region, and the equipment is available and acquired more quickly.

1.5 Implement Work-Arounds to Address Changes to Operations Processes, etc.

Service Provider will use its experience in varied operational processes to achieve quick recovery results. As recovery and restoration efforts near completion, all operational processes in effect that differ from standard Province processes will be reverted to standard Province processes, where possible.

1.6 Operate and Report on Services Within Limitations of Work-Arounds

The Service Provider's Operation Centre will report the status of the recovery and consult with the Province with respect to process changes in order to help ensure that the Province has a thorough understanding of progress and has a collaborative role in the recovery and restoration operations.

2. RESERVE CAPACITY

In respect of reserve capacity, "Service Provider Efforts" will include without limitation the following:

2.1 Electricity - VA Gap between Province Commitment and Usage

The VA gap between the Province's VA commitment and the Province's usage of electricity represents the reserve capacity available to the Province and any Client at each STMS Data Centre that is not affected by a Disaster

The Service Provider will maintain, in confidence, a monthly estimation of the available data centre resources (*e.g.*, for floor space and power) at its other Canadian data centres and those of DC Subcontractor to lessen the chance that in the event of a Disaster proper decisions and actions will be delayed.

2.2 Virtual Hosts - Windows, UNIX and Linux

Service Provider will operate its Virtual Servers at the Server Farm Threshold and the Physical Host Threshold (each as defined in the Virtual Hosting Services SOW), which is at a capacity utilization of approximately a 75% average. Inherent in the design of Virtual Server technologies is the ability to set resource limits on individual guest servers. In the event of a Disaster, the Service Provider will review all guest servers and modify resource limits on guest servers supporting non-mission critical or non-business critical workload and make recommendation, as necessary, to the Province identifying some non-critical guest servers to be shut down. With the Province's approval, such non-critical virtual guest servers will be temporarily shutdown. Service Provider will then recover impacted mission critical and business critical workloads into these physical host servers having additional capacity available for utilization, including use of any available capacity that exceeds the Server Farm Threshold. In addition, the Service Provider will use the capacity of supplemental physical servers as soon as they are acquired by the Service Provider..

2.3 Physical Hosts Windows, UNIX and Linux

Service Provider does not intend to, on its own, maintain a shelf supply of physical servers in the data centres so there is no assured reserve capacity. However, if there are any available servers as a result of in-process orders or decommissioning, Service Provider will use these to supplement its recovery capabilities until additional equipment is received from suppliers. Service Provider will also use any physical servers that the Province designates as able to be repurposed from their normal usage (such as development servers).

2.4 Storage

Minimum operational storage reserves are:

- Tier 1: 3 TB
- Tier 2: 26.5 TB
- Tier 3: 42 TB

The Service Provider acknowledges that its supplier has committed to have up to 20TB of additional Tier 1 storage available for shipment within 30 days Business Days. Until delivery, Service Provider will substitute available Tier 2 storage.

The Service Provider acknowledges that its supplier has committed to have up to 100TB of additional Tier 2 and 3 storage available, in aggregate, for shipment with 10 Business Days.

Service Provider will also use any storage that can be re-purposed by the Province through deletion of non-essential (as determined by the Province) data, and which data can be restored from backup at a later date.

2.5 Network Attached Storage

Service Provider will not be maintaining a shelf supply of Network Attached Storage ("**NAS**") in the data centres so there is no assured reserve capacity. However, if there are any available NAS servers as a result of in-process orders or decommissioning, Service Provider will use them to supplement its recovery capabilities until additional equipment is received from suppliers. Service Provider will also use any NAS that can be re-purposed by the Province by deletion of non-essential (as determined by the Province) data, and which data can be restored from backup at a later date.

2.6 Network Switches

Service Provider will not be maintaining a shelf supply of network switches in the data centres. Most network switches are anticipated to run near full port occupancy, though a few ports may be available. Network switches are procured as the Province submits service orders or as additional capacity is required for Transformation. However, if there are any available network switches as a result of in-process orders or decommissioning, Service Provider will use these to supplement recovery capacity until additional equipment can be received from suppliers.

Service Provider will be able to supply up to 192 additional switch ports within 10 Business Days, which is adequate for support of approximately 48 additional servers. Service Provider will be able to increase the number of additional switches if the Province believes there will be a need for more than 48 additional servers.

Appendix D - Mainframe Disaster Recovery Service

The Mainframe Disaster Recovery Service is the planning and test of the system-level recovery of the operating system in the primary compute environment or at the Disaster recovery site (the "**Disaster Recovery Site**") and, is the recovery and restoration of availability of the Mainframe System Software in the event of a disruption, loss or Disaster.

This service provides for:

- the recovery and restoration of the Mainframe System Software and availability so the Province can proceed with the restoration of Applications and data;
- Planning, documentation, testing the operating system recovery procedures, and restoring the Mainframe System Software in the At issue for Inquiry or the Disaster Recovery Site.

1.1 Disaster Recovery Planning

The Service Provider will provide disaster recovery services at a level of performance which will allow the Province to restore and/or continue the functions of Applications after a declared Disaster or data centre failure.

Disaster Recovery Planning identifies, develops, documents and supports proactive activities that mitigate risk and provide plans, information, tools, and coordinated procedures to appropriately respond to and recover the operating system in the primary compute environment or at the Disaster recovery centre.

Disaster Recovery Planning Tasks and Functions	Responsibility	
	Province	Service Provider
Document, test and update procedures in a Service Provider Disaster Recovery Plan necessary for the secure, successful and coordinated recovery of the Mainframe System Hardware and the Mainframe System Software (to be referred to herein as the "**Mainframe System Software**").		R
Define the system resources, human resources, and physical resources and any other resource required to securely recover the operating system and incorporate the resource requirements information into the Service Provider Disaster Recovery Plan (DRP).		R

Disaster Recovery Planning Tasks and Functions	Responsibility Province	 Service Provider
Develop the Service Provider Disaster Recovery Plan to support and achieve RTOs that do not exceed: • 48 elapsed hours immediately from the date and time there has been a data centre failure to restore 100% of production function and production data and 50% of processing capacity; • 48 elapsed hours from the date and time of Disaster declaration by the Province to restore 100% of production function and production data and 50% of processing capacity; • 10 elapsed calendar days from the date and time of Disaster declaration by the Province to restore 100% of development functions and data; and • in 40 elapsed calendar days from the date and time of Disaster declaration by the Province to restore 100% of processing capacity.		R
Provide Service Provider Disaster recovery awareness and training for Mainframe System Software and provide the Province written confirmation, as documented in 'STMS Hosting Services SOW 8 – Business Continuity and Disaster Recovery Services'.		R
Develop and include in the Service Provider Disaster Recovery Plan the interactions and integration of the Service Provider Disaster Recovery Plan with the Service Provider Operations Centre Plan.		R
Add the Service Provider Disaster Recovery Plan to the list of approved Service Provider Disaster Recovery Plans.		R

1.2 Disaster Recovery Test

The Disaster Recovery Test may also be known or referred to as the Information Technology Recovery Exercise (ITRE). The ITRE is the testing process that validates the Service Provider Disaster Recovery Plan ("**DRP**") and demonstrates successful recovery and restoration of the Mainframe System Software. The recovery test is used to improve the plan's state of preparedness, accuracy, and viability. Testing also validates the predefined time and resources to recover the Mainframe System Software and facilitates the improved availability of the

Mainframe System Software if a disruption or failure occurs. The recovery test familiarizes response personnel and participants by validating response activities, roles, and procedures. Information Technology Recovery Exercises are scheduled at least once annually and may be coordinated in conjunction with other operating system recoveries or DRP/BCP testing.

The Province will be responsible for identifying Application code and Application data that is required for recovery and for coordinating Application testing activities. The Service Provider will manage the custody and secure shipment of tapes that are necessary to restore the Application code and Application data. In all cases the Service Provider will provide sufficient operational support staff to manage and coordinate the recovery and restoration and to enable or assist the recovery and restoration of the Application code and Application data. A minimum and continuous 48-hour test block is allocated to the recovery testing of the Mainframe System Software, Application code and Application data.

In the event that the Disaster Recovery Site becomes unavailable for the test, the Service Provider will manage the custody and secure shipment of tapes that are necessary to restore the Application code and Application data.

Disaster Recovery Test Tasks and Functions	Responsibility	
	Province	Service Provider
Establish test objectives and review with the Province to ensure that the agreed scope of the test is understood.		R
Plan, arrange and conduct an annual Mainframe System Software recovery test, executing the procedures as outlined in the Disaster Recovery Plan (DRP) at the Disaster Recovery Site.		R
During the testing activities related to the Mainframe System Software recovery; recover, operate, maintain, coordinate and support the availability of the Mainframe System Software, hardware and related communications capability at the Disaster Recovery Site.		R
Schedule the test dates with Province input.		R
Approve the test dates.	R	
Develop a Province client guide or any Recovery Exercise related document references, except the Service Provider Disaster Recovery Plan(s), that may be required by the Province to effect the participation of the Province in a Recovery Exercise.	R	

Disaster Recovery Test Tasks and Functions	Responsibility Province	 Service Provider
Participate with the Province to develop a Province client guide or any Recovery Exercise related document references that may be required by the Province to effect the participation of the Province in a Recovery Exercise, especially where the reference information can only be provided or confirmed by the Service Provider.		R
Coordinate the Province participation in the Recovery Exercise, as may be necessary.	R	
Integrate and participate in the coordination of Province participation in the Recovery Exercise, as may be necessary, including pre and post test meetings with the Province.		R
Establish and validate network communications from SPAN/BC to the Disaster Recovery Site.	R	
Consult with the Province to validate the network communications from SPAN/BC to the Disaster Recovery Site.		R
Provide WAN connectivity from the Service Provider's network to the Disaster Recovery Site.		R
Activate functional communications network during Disaster Recovery Test.	R	
Conduct both pre and post test meetings with the Province.		R
Coordinate Application recovery test activities.	R	
Identify, retrieve and recover the appropriate version of the Mainframe System Software as defined in the Service Provider Disaster Recovery Plan.		R
Verify the Mainframe System Software at the Disaster Recovery Site is fully functional and available for Application recovery and testing.		R
Provide experienced and qualified recovery specialists as required to conduct the test. This would include technical and support staff to assist the Province Application recovery.		R
Perform and verify Application recovery.	R	

Disaster Recovery Test Tasks and Functions	Responsibility Province	 Service Provider
At the conclusion of the test at the Disaster Recovery Site, destroy residual data or make it inaccessible by wiping the media in compliance with US Department of Defense Standard 5220.22-M (c) Clearing and Sanitization Matrix, or equivalent.		R
Identify and recommend procedural or technical changes that could expedite recovery and restoration or improve the Service Provider Disaster Recovery Plan.		R
Within 30 days following the completion of the annual test, provide the Province with: • written and signed confirmation that the disc media at the Disaster Recovery Site has successfully been wiped; • a formal and signed copy of the Mainframe Disaster Recovery Executive Summary and ITRE Results, including known recommendations, in keeping with the requirements and responsibilities as documented in the STMS Hosting Services SOW 8 – Business Continuity and Disaster Recovery Services; • a post exercise ITRE Issue List (in a format to be agreed by the Service Provider and the Province) documenting issues to be remedied by the Service Provider and/or the Province or the Clients responsible for recovering the Applications and data, in keeping with the requirements and responsibilities as documented in the STMS Hosting Services SOW 8 – Business Continuity and Disaster Recovery Services; and • an updated Service Provider Disaster Recovery Plan for Managed Mainframe Services, including new or updated Appendices, in keeping with the requirements and responsibilities as documented in the STMS Hosting Services SOW 8 – Business Continuity and Disaster Recovery Services.		R

Disaster Recovery Test Tasks and Functions	Responsibility Province	 Service Provider
Receive and review the reports, evidence summaries, recommendations, issues list and any additional related submissions of updates.	R	S
Approve or reject improvements or recommendations that require additional funding, policy changes, or specific approvals by others.	R	I

1.3 Mainframe Disaster Recovery

The Service Provider will predetermine and establish the Disaster Recovery Site in Canada. The Disaster Recovery Site will include the use of shared and dedicated resources that will be activated for recovery and restoration. These shared resources are qualified, trained and equipped to successfully execute the Service Provider Disaster Recovery Plan.

If sufficient resources at the Disaster Recovery Site are not available to the Province and the Service Provider during a Disaster, e.g. because the resources are being used by another user of the Disaster Recovery Site, the Service Provider will proactively and vigorously use prudent and commercially reasonable efforts to acquire alternate qualified, trained and equipped recovery resources.

If the Disaster Recovery Site is not available, in whole or in part, to the Province and the Service Provider during a Disaster, e.g. because the Disaster Recovery Site is being used by other users of the Disaster Recovery Site, then the Service Provider will proactively and vigorously use prudent and commercially reasonable efforts to acquire alternate recovery resources in Canada, and, then, if no alternate recovery resources or equally adequate alternate facility is available in Canada, the United States or other countries with permission of the Province.

Mainframe Disaster Recovery Tasks and Functions	Responsibility Province	 Service Provider
Recover and restore the Mainframe System Software in the or at the Disaster Recovery Site. At issue for Inquiry		R
Recover and restore user catalogues for the restoration of the Client Applications and Application data.		R
Verify synchronization of the Client Applications and Application data with operating system files or any catalogue restore.	R	

Mainframe Disaster Recovery Tasks and Functions	Responsibility Province	 Service Provider
Restore the Applications and Application data.	R	
In the event that the Disaster Recovery Site is not available, manage the secure custody and shipment of tapes that are necessary to restore the Client Applications and Application data.		R
In the event where the Disaster Recovery Site becomes unavailable, the Service Provider will proactively and vigorously use prudent and commercially reasonable efforts to acquire alternate recovery resources in Canada, and, then, if no alternate recovery resources or equally adequate alternate facility is available in Canada, the United States or other countries with permission of the Province.		R
Provide permission to the Service Provider to acquire the alternate recovery resources outside of Canada, including in priority; the United States or other countries, in the event that the designated Disaster Recovery Site is not available and Service Provider efforts to acquire the alternate recovery resources in Canada are not successful.	R	
Securely ship any removable media to and from the Disaster Recovery Site.		R

Appendix E – Sample SOW for Disaster Recovery Plan Development

Sample Only
Contents and specifics are included as illustration and informational purposes only and not intended to preclude the negotiated development of business specific Statements of Work

(Subject to update, as may be deemed by Service Provider and agreed by the Province to be appropriate)

Statement of Work

for

Disaster Planning Services

For

"_application/system_"

TABLE OF CONTENTS

Note: Use the "Word Find and Replace" feature to find "_application/system_" and "_RTO_" (including the double quotes). Replace these with the name of the application and or system that this SOW relates to and the specific RTO required. Then delete this note in is entirety.

SCHEDULE 7

LANGUAGE OF SERVICES

Nil

SCHEDULE 8

SERVICE LOCATIONS

1. Data Centres.

1.1 ***Province*:** Province owned or controlled data centres:

S. 15

(collectively, the "**Province Data Centres**")

1.2 ***Service Provider*:** Service Provider owned or controlled data centres:

STMS Interior Data Centre

STMS Calgary Data Centre

(together, the "**STMS Data Centres**")

S. 15

(collectively, with the STMS Data Centres, the "**Service Provider Data Centres**")

The Service Provider will perform Services for the Province from the Service Provider Data Centres identified above (all of which data centres are leveraged facilities, within which services

will be provided for other entities).

1.3 ***Province Remote Infrastructure Server Locations*:**

S. 15

S. 15

(collectively, the "**Remote Infrastructure Server Locations**")

1.4 ***Province Remote Application Server Locations*:**

S. 15

S. 15

S. 15

(collectively, "**Remote Application Server Locations**")

1.5 ***Service Provider Other*:**

S. 15

3. General Provisions.

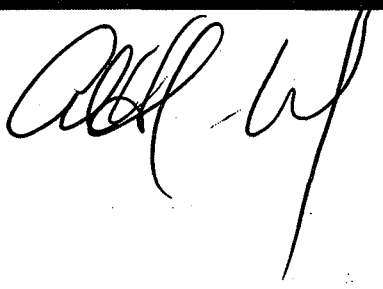
3.1 Certain Service Locations from which the Services are provided will change in accordance with the Transformation Plan and the Business Continuity Plan (for example, over time Province equipment will be moved from the Province Data Centres listed in Section 1.1 above to the STMS Data Centres). The Province's Approval of the Transformation Plan and Business Continuity Plan will constitute Approval, for the purposes of the Agreement, of any changes in Service Locations provided that they are completed in accordance with the Approved Transformation Plan and Approved Business Continuity Plan.

SCHEDULE 9

TRANSFORMATION SOW

See attached.

[redacted]



50652395.10

Table of Contents

1. INTRODUCTION

1.1 Definitions

Capitalized words used in this Statement of Work ("**SOW**") shall incorporate the meanings given to such words in the Agreement. In the event that a term is not defined in the Agreement, it shall have the meaning provided in Appendix A (*Definitions*) of this SOW or in the body of this SOW.

1.2 Purpose of this Document

1.2.1 Purpose of this Document

This SOW describes the Transformation Projects to be performed by the Service Provider under the Agreement and responsibilities of the Service Provider and the Province in connection therewith.

This SOW must be read in conjunction with the Transformation Plan attached as Schedule 10 (*Transformation Plan*) to the Agreement. The Transformation Plan sets out the detailed schedule of tasks for the performance of the Transformation Projects described in this SOW.

1.2.2 Appendices

The following Appendices are attached to and form part of this SOW, whether or not they are specifically referred to in this SOW:

- Appendix A – Definitions
- Appendix B – Intentionally Deleted
- Appendix C – Manual Outline
- Appendix D – Province Freeze Periods

1.3 Related SOWs

The Parties acknowledge and agree that this SOW is subject to the provisions of the Agreement and Schedules to the Agreement. However, the Parties have identified the following SOWs or Schedules to the Agreement as being important to the understanding of Services set forth in this SOW:

- Data Centre Services SOW
- Business Continuity and Disaster Recovery Services SOW
- Security SOW
- Service Management SOW
- Managed Mainframe Services SOW
- Server Management Services SOW
- Managed Storage and Managed Backup Services SOW

1.4 Interpretation

Statements or references in this SOW or the Transformation Plan to the Service Provider providing written notification to the Province when a deliverable or milestone (together, a "milestone") has been completed or achieved shall not alter the Service Provider's obligation to achieve the milestone by the date set out in the Transformation Plan nor require the Province to agree that any such milestone has been completed or achieved.

The Parties acknowledge and agree that each milestone (whether delivered individually or along with other milestones) will be deemed completed or achieved once such milestone has been Approved by the Province, provided that, the Province shall not be required to approve the milestones set forth in Sections 3 and 4 of this SOW or milestones that are internal to the Service Provide and do not impact the Province.

2. TRANSFORMATION OUTCOMES

The Transformation Program is a group of 13 interrelated Transformation Projects described in the following sections of this SOW:

Section 3	-	Service Provider Business Operations Implementation
Section 4	-	Office Facilities
Section 5	-	STMS Data Centres
Section 6	-	Network LAN/WAN
Section 7	-	Service Management
Section 8	-	Mainframe Services Migration Project
Section 9	-	Server Systems Management Transformation
Section 10	-	Virtualization Assessment and Migration Planning
Section 11	-	Field Services
Section 12	-	Storage and Backup
Section 13	-	After Hours Service Desk
Section 14	-	Security
Section 15	-	Virtualization and Migration

The Transformation Projects support the achievement of the objectives set out in Section 1.13 of the Agreement. The Transformation Projects will achieve the following:

(a) the STMS Data Centres will be constructed in the Interior of British Columbia and in Calgary, Alberta in accordance with Section 5 (*STMS Data Centres Transformation Project*) of this SOW. The STMS Data Centres will comply with the requirements of the Agreement relating to availability, reliability and redundancy and will be available to provide Services to the Province in accordance with Data Centre Services SOW;

(b) the Services will be provided from facilities and using Systems that comply with the Security SOW attached to the Agreement;

(c) implementation of Service Provider software tools and processes for the management of Province Systems in accordance with Section 7 (*Service Management*) of this SOW;

(d) installation and implementation of network facilities linking the STMS Data Centres with the Province and other Service Provider Support Locations in accordance with Section 6 (*Network LAN/WAN*) of this SOW;

(e) migration of the Province's mainframe services to a new hardware and software environment in the in accordance with Section 8 (*Mainframe Services Migration*) of this SOW;

(f) migration of Province Servers to new hardware and software environments in the STMS Data Centres, and virtualization of those Servers to the extent planned in accordance with Section 10 (*Virtualization Assessment and Migration Planning Project*) of this SOW;

(g) migration of the Managed Storage and Managed Back-up Services to new hardware and software environments in the STMS Data Centres in accordance with Section 12 (*Storage and Backup*) of this SOW; and

(h) installation and implementation of Service Provider office facilities and business operations to support a Transformation Program Office and other business activities necessary to support the Agreement in accordance with Section 3 (*Service Provider Business Operations Implementation*) and Section 4 (*Office Facilities Transformation Project*) of this SOW.

The objectives of the Transformation Program will be supported by:

(i) an economic model, set out in Schedule 23 (*Fees*) of the Agreement, that facilitates and encourages growth by the Province and participation and growth by the Broader Public Sector;

(ii) governance structure, reviews, processes and remedies that enable constructive discussion and collaboration, timely decision-making and the achievement of milestones; and

(iii) the commitment of the Parties to the success of the Transformation Program.

The Transformation Projects are presented in an order that is logical from a project management perspective, however, such order does not reflect the importance of one project over another.

3. SERVICE PROVIDER BUSINESS OPERATIONS IMPLEMENTATION

"Business Operations" refers to the underlining business processes and tools that enable the Service Provider to provide services to its clients. The functions typically provided by the

Service Provider to its customers as "Business Operations" include client care, financial management and program management.

Pursuant to Business Operations Transformation Project, the Service Provider will:

(a) establish processes and tools to operate the Service Provider Business Office and Program Management Office and to manage client care; and

(b) refine the Transformation Plan.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Service Provider Business Operations Implementation	**Establish Program Management Office and implement required governance processes including SLA reporting, project status reporting, project phase gate reviews, issue and risk management**		N/A	Month 1, April, 2009 (processes available for Province review) Month 2, May, 2009 (PMO senior personnel are assigned) Month 3, June, 2009 (governance processes are refined with Province input and fully operational) Month 7, October, 2009 (for new SLA reporting)	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
	Establish Business Office and implement required processes such as billing		N/A	Month 1, April 2009 Month 7, October, 2009 (for unit billing)	**Referenced business processes are operational** **Business Office is organized and senior personnel assigned**
	Implement Service Provider client care processes		N/A	Month 1, April, 2009	**Communication Plans are executed and Service Excellence Voice of the Client survey capability is available**
	Refine the Transformation Plan		N/A	Month 3, June, 2009 (for initial refinement)	**Transformation Plan ready to be reviewed with Governance Committees**

3.1 Establish Program Management Office

The Service Provider will establish a program management office (the "**Program Management Office**") through which the Service Provider will:

(a) produce Service Level reports;

(b) implement, at the Service Provider's expense, the Governance Process described in the Agreement;

(c) establish and operate an issue / risk management process; and

(d) provide project status reporting;

in support of the Transformation Projects and the Service Provider's operations.

The Service Provider will provide written notification to the Province when the Program Management Office is operational.

3.2 Establish Business Office

The Service Provider will establish a business office (the "**Business Office**") through which the Service Provider will, among other things:

(a) implement and manage the Service Provider's participation in the Change Order Process; and

(b) implement and manage billing processes and financial reporting,

in accordance with the Agreement.

The Service Provider will provide written notification to the Province when the Business Office is operational.

3.3 Implement Client Care Processes

The Service Provider will prepare and implement the following client care processes:

(a) a communications plan for internal Service Provider communications; and

(b) a communications plan between Service Provider and the Province in accordance with Schedule 17 (*Communications Plan and Process*) of the Agreement.

The communications plan will incorporate the Service Provider's "Voice of the Client" process. The Service Provider's Voice of the Client process allows the Province to participate in a Service Excellence survey or interview process, at least once per year. The Province may also initiate the survey process on its own initiative. Interviews are face-to-face discussions among an independent representative from the Service Provider's Service Excellence team and three to five representatives of the Province selected by the Province. The interviews typically last one hour and include open-ended questions about the Service Provider's performance, deliverables and service quality as well as past challenges, current expectations and future objectives.

3.4 Refine Transformation Plan

The Service Provider and the Province have prepared the Transformation Plan attached to the Agreement as Schedule 10 (*Transformation Plan*).

Subject to the provisions of Article 6 (*Transformation*) of the Agreement, the Service Provider and the Province will collaborate on the initial refinement of the Transformation Plan (as refined, the "**Revised Transformation Plan**") as follows:

(a) the Service Provider and the Province will collaborate to identify required revisions to the Transformation Plan, if any, with consideration for the timing constraints described in Appendix D (*Province Freeze Periods*) and will resolve any conflicts with these constraints to the satisfaction of the Province;

(b) the Service Provider will prepare and deliver to the Province a Revised Transformation Plan for the Province's review; and

(c) the Service Provider and the Province will approve the Revised Transformation Plan, as presented by the Service Provider or as the Parties otherwise agree to amend the Transformation Plan in accordance with the Governance Process.

Ongoing refinements of the Revised Transformation Plan will also be completed as set out above. For greater certainty, in this SOW, "Transformation Plan" refers, at any time, to: (i) the Transformation Plan attached as Schedule 10 (*Transformation Plan*) to the Agreement; or (ii) the Revised Transformation Plan, whichever is in effect at such time.

4. OFFICE FACILITIES TRANSFORMATION PROJECT

Pursuant to the Office Facilities Transformation Project, the Service Provider will establish office space for the Service Provider Personnel.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Office Facilities Transformation	**Service Provider Office Space**	Preparation of Service Provider office facilities	N/A	Month 3, June, 2009	**Office space outfitted and ready for Service Provider Personnel**

4.1 Use of WTS Office Facilities and Assets

The Transitioning Employees will remain in the WTS facilities and the Service Provider will perform the Services from the WTS facilities until the Service Provider Office Facilities are prepared and ready for occupancy (provided that the Service Provider Office Facilities shall be ready for occupancy and the Transitioning Employees and any Service Provider managers shall move from the WTS Facilities to the Service Provider Office Facilities no later than the end of month three of the Term). During the period until the Service Provider Office Facilities are ready for occupancy, the Transitioning Employees will continue to:

- use the same office facilities as the Transitioning Employees were using immediately prior to the Hand-Over Date when they were employees of the Province (collectively, the "**WTS Office Facilities**"); and

- have use of all Province infrastructure and tools to perform the Managed Services as the Transitioning Employees were using immediately prior to the Hand-Over Date when they were employees of the Province.

The Service Provider will cause the Transitioning Employees and all Service Provider managers who access the WTS Office facilities to comply with all Province Policies relating to access, security, safety, operations and facilities procedures relating to the WTS Office Facilities.

The Province will:

(a) for the three month period following the Hand-Over Date, make available:

(i) the WTS Office Facilities for the Transitioning Employees and Service Provider managers (approximately 100 workspaces and 9 offices); and

(ii) the tools being used by the Transitioning Employees prior to the Hand-Over Date, the IT infrastructure and network connectivity to allow the Transitioning Employees and the four Service Provider managers to perform the Managed Services while located at the WTS Office Facilities in the same manner as the Transitioning Employees were performing such services immediately prior to the Hand-Over Date;

(b) for up to ninety days following the Hand-Over Date, make available the cellular telephones, pagers and similar communication devices provided by the Province to the Transitioning Employees immediately prior to the Hand-Over Date (such cellular telephones, pagers and similar communication devices will be provided to allow the Transitioning Employees to perform the Managed Services in the same manner as such services were being provided by them immediately prior to the Hand-Over Date only); and

(c) cause the telephone numbers of such cellular telephones, pagers and similar communication devices to be assigned to the Service Provider when the Service Provider replaces the Province supplied devices with similar devices belonging to the Service Provider.

4.2 Preparation of Service Provider Office Facilities

The Service Provider will prepare the Service Provider Office Facilities for Service Provider Personnel (which, for greater certainty, includes the Transitioning Employees) who will be involved in providing Services to the Province. The Service Provider will provide written notification to the Province when the Service Provider Office facilities are ready for Service Provider Personnel.

4.3 Service Provider Exit from WTS Office Facilities

The Service Provider will:

(a) cause the Transitioning Employees and Service Provider managers (the Service Provider Personnel) at the WTS Office Facilities to leave the WTS Office Facilities no later than the end of month three of the Term;

(b) in connection with the departure of the Service Provider Personnel from the WTS Office Facilities, transition from the WTS Exchange mail service, personal computers and LAN connectivity to the Service Provider's personal computers, Exchange mail service and LAN connectivity; and

(c) following the departure of the Service Provider Personnel from the WTS Office Facilities, leave the WTS Office Facilities in the same condition as they were immediately prior to the Hand-Over Date, normal wear and tear excepted.

After the third month of the Term of the Agreement, the Province will make available to the Service Provider Personnel, at the WTS Office Facilities, for the Service Provider's use in the performance of the Managed Services, the following:

- IDIR IDs and Exchange mailboxes (shared generic email boxes only) for select Service Provider employees as required to perform the Managed Services; and

- Network access for Service Provider Personnel required to work at WTS facilities in order to perform the Managed Services (for example, to respond to incidents, to carry out preventive maintenance, for the delivery of new additional services).

5. STMS DATA CENTRES TRANSFORMATION PROJECT

Pursuant to the STMS Data Centres Transformation Project, the Service Provider will cause two data centres to be constructed, one in Calgary, Alberta and one in the interior of British Columbia.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Data Centre Facilities Transformation	**STMS Calgary Data Centre**	STMS Data Centre Availability Date		Month 8, November 1, 2009	**Customer Environment for Managed Services available to Service Provider for installation of Managed Services.**
		Initial Production Services		Month 10, January, 2010	**Service Provider providing Managed Services to the Province**
	STMS Interior Data Centre	STMS Data Centre Availability Date		Month 25, April 1, 2011	**Customer Environment for Managed Services available to Service Provider for installation of Managed Services.**
		Initial Production Services		Month 27, June, 2011	**Service Provider providing Managed Services to the Province**

5.1 Introduction

5.1.1 Construction of STMS Data Centres

Under the STMS Data Centres Transformation Project, the Service Provider will cause the following to be completed on or before the STMS Data Centre Availability Dates set forth below:

(a) the construction of a new data centre facility located in the Interior of British Columbia with a minimum initial capacity of 1,800,000 VAs and a minimum potential VA capacity of 3,600,000 VAs; and

(b) the expansion of an existing data centre facility located in Calgary, Alberta with a minimum initial capacity of 1,800,000 VAs and a minimum potential VA capacity of 7,200,000 VAs.

5.1.2 Requirements

The STMS Data Centres, and each STMS Data Centre will:

(a) at a minimum, comply with the requirements of the Agreement including the STMS Data Centre requirements set out in Appendix G (*Data Centre Requirements*) of the Data Centre Services SOW (the "**Specifications**") of the Agreement;

(b) be constructed in accordance with the timeline set forth in the Transformation Plan, including the construction milestones identified in this SOW; and

(c) be available for the provision of Data Centre Services by the Service Provider to the Province not later than as documented in Table 1 – STMS Data Centre Availability Dates below.

Table 1 – STMS Data Centre Availability Dates

STMS Interior Data Centre **STMS Data Centre Availability Date**	**STMS Calgary Data Centre** **STMS Data Centre Availability Date**
April 1, 2011	November 1, 2009

5.1.3 Completion

For the purposes of this SOW, the construction of each STMS Data Centre will be deemed to be "complete" and the STMS Data Centre Availability Date Milestone (see table above) will have been met when:

(a) the construction of the STMS Data Centre has been completed in accordance with the requirements of the Specifications;

(b) the STMS Data Centre has been built in compliance with Applicable Laws; and

(c) the Customer Environment for Managed Services is completed and meets the requirements set forth in the Data Centre Services SOW.

Note to Draft: EDS is proposing a new definition for "Customer Environment for Managed Services" as this term is not defined in the Data Centre Services SOW.

The Service Provider will cause its Data Centre Services Subcontractor to certify on or prior to the applicable STMS Data Centre Availability Date (the "**STMS Data Centre Certification**") that the conditions set out in paragraphs 5.1.1(a) - (b) have been satisfied. The STMS Data Centre Certification will be signed by a senior officer of the Data Centre Services Subcontractor and will include, as an attachment and to the extent available, copies of any required occupancy certificates issued by Governmental Authorities in the locality in which such STMS Data Centre is located.

Nothing in this SOW or the Agreement will require the Province to move in to the Customer Environment for Managed Services of an STMS Data Centre before the applicable STMS Data Centre Availability Date, even if the STMS Data Centre is available as a result of the early build and completion of such STMS Data Centre.

5.2 STMS Interior Data Centre

The Service Provider will cause the STMS Interior Data Centre to be constructed in accordance with the Specifications, the provisions of this SOW and the Transformation Plan.

The Province acknowledges that the STMS Interior Data Centre is a leveraged facility and that the Service Provider will utilize the STMS Interior Data Centre to provide services to the Province and other customers.

5.2.1 Completion of Purchase

The Service Provider will cause its Data Centre Services Subcontractor (or an affiliate of the Data Centre Services Subcontractor) (the "**Buyer**") to complete the purchase of the land and/or building at the location identified in Schedule 8 (*Service Locations*) to the Agreement for the construction of the STMS Interior Data Centre in accordance with the Transformation Plan.

The Service Provider will provide the Province with a certification (the "**Certification**") in the form of the Milestone Deliverable Certification attached to this SOW as Appendix E (*Milestone Deliverable Certification*) when:

(a) the Buyer has entered into an agreement of purchase and sale with the seller to purchase the site (the "**Site**") for the STMS Interior Data Centre site; and

(b) the agreement of purchase and sale forms a binding obligation of the Buyer and the seller for the purchase and sale of the Site, subject to the conditions set out in the Milestone Deliverable Certification attached to this SOW as Appendix E (*Milestone Deliverable Certification*).

5.2.2 Interior Construction Milestones and Reporting

The Service Provider will report on the achievement of the following milestones (the "**Interior Milestones**") related to the construction of the STMS Interior Data Centre in accordance with Section 5.4 (*Reporting and Transformation Credits*) of this SOW:

(a) Site Purchase

(b) Conceptual Design Complete

(c) Earthworks

- Earthworks permit issued
- Start site grading and construction of access roads

(d) Building permits issued:

- Building and Equipment Yard Foundation Work Starting
- Start building foundation and major equipment pad and diesel fuel yard layout
- Electrical and mechanical rough-in
- Concrete formwork
- Pour and finish Slab

(e) Structural Steel Work

- Start erecting structural steel for building walls and roof

(f) Structural Framing Complete

- Start cladding exterior walls and enclosing roof

(g) Building Shell and Roof Complete

- Start interior build out
- Framing demising walls, drywall installation, electrical distribution system and mechanical systems rough-in

(h) Major Equipment on Site

- Transformers
- UPS equipment
- PDUs
- Diesel generators
- Fuel oil tanks
- HVAC equipment
- Interior work continuing

(i) Major Equipment Placed

(j) Major Equipment Installation nearing completion:

- Interior works continuing (architectural finishes, millwork, hardware)

(k) Start Commissioning Major Equipment

- Interior works substantially complete
- Commissioning of security, fire alarm and building automation system and controls underway

(l) Commissioning substantially complete

- Begin Province space improvements

- Final Cleaning

(m) Project complete, ready for customer move in

The reporting to be provided by the Service Provider to the Province will identify progress of the construction of the STMS Interior Data Centre against the Interior Milestones above including whether or not such Interior Milestones are on schedule or delayed and the achievement of such Interior Milestones in accordance with the Transformation Plan.

The Interior Milestones identified above are provided for information and reporting purposes only. The Parties acknowledge that the Interior Milestones are subject to change in the course of the construction of the STMS Interior Data Centre, provided that no change in the Interior Milestones shall be effective to change the STMS Data Centre Availability Date for the STMS Interior Data Centre.

5.2.3 Availability of STMS Interior Data Centre at STMS Data Centre Availability Date

The Service Provider will provide the STMS Data Centre Certification to the Province on or prior to the STMS Data Centre Availability Date for the STMS Interior Data Centre.

5.2.4 Security Threat Risk Assessment for STMS Interior Data Centre

The Service Provider will conduct a Security Threat Risk Assessment in respect of the STMS Interior Data Centre in accordance with Schedule 24 (*Privacy Obligations*) of the Agreement within thirty days of the STMS Data Centre Availability Date for the STMS Interior Data Centre.

5.2.5 STMS Interior Data Centre Requirements Verification

The Service Provider will complete the Data Centre Requirements Verification described in Section 5.4 of the Data Centre Services SOW to verify that the STMS Interior Data Centre meets the data centre infrastructure requirements described in Appendix G (*Data Centre Requirements*) of the Data Centre Services SOW of the Agreement. The Data Centre Requirements Verification in respect of the STMS Interior Data Centre will be completed in accordance with the schedule described in the Transformation Plan.

5.2.6 Provision of Services

The Service Provider will prepare the Customer Environment for Managed Services to enable the Service Provider to provide the Managed Services as described in Section 6 (*Network LAN/WAN*), Section 9 (*Server Systems Management Transformation*), and Section 12 (*Storage and Backup*) of this SOW.

The Service Provider will provide Services from the STMS Interior Data Centre to the Province as follows:

(a) as Applications (and their associated data) are migrated to the STMS Interior Data Centre in accordance with Section 15 (*Virtualization and Migration Project*) of this SOW; and

(b) in response to the Service Request process described in the Service Management SOW.

5.3 STMS Calgary Data Centre

The Service Provider will cause an expansion to the existing STMS Calgary Data Centre in accordance with the requirements of the Agreement and the Transformation Plan. The STMS Calgary Data Centre will be available for the provision of Managed Services to the Province in accordance with the Transformation Plan.

The Service Provider will utilize the STMS Calgary Data Centre in providing the Managed Services to the Province and for providing the Services described in the Data Centre Services SOW to the Province if the Province elects to receive Data Centre Services from the Service Provider at the STMS Calgary Data Centre.

The Province acknowledges that the STMS Calgary Data Centre is a leveraged facility and that the Service Provider will utilize the STMS Calgary Data Centre to provide services to the Province and other customers.

5.3.1 Calgary Construction Milestones and Reporting

The Service Provider will report on the achievement of the following milestones (the "**Calgary Milestones**") related to the construction of the STMS Calgary Data Centre in accordance with Section 5.4 (*Reporting and Transformation Credits*) of this SOW:

(a) Major Equipment Installation nearing completion:

- Interior works continuing (architectural finishes, millwork, hardware)

(b) Start Commissioning Major Equipment

- Interior works substantially complete
- Commissioning of security, fire alarm and building automation system and controls underway

(c) Commissioning substantially complete

- Begin Province space improvements
- Final Cleaning

(d) Project complete, ready for customer move in

The reporting to be provided by the Service Provider to the Province will identify progress of the construction of the STMS Calgary Data Centre against the Calgary Milestones above including

whether or not such Calgary Milestones are on schedule or delayed, and the achievement of such Calgary Milestones in accordance with the Transformation Plan.

The Calgary Milestones identified above are provided for information and reporting purposes only. The Parties acknowledge that the Calgary Milestones are subject to change in the course of the construction of the STMS Calgary Data Centre, provided that no change in the Calgary Milestones shall affect or change the STMS Data Centre Availability Date for the STMS Calgary Data Centre.

5.3.2 Availability of STMS Calgary Data Centre at STMS Data Centre Availability Date

The Service Provider will provide the STMS Data Centre Certification to the Province on or prior to the STMS Data Centre Availability Date for the STMS Calgary Data Centre.

5.3.3 Security Threat Risk Assessment for STMS Calgary Data Centre

The Service Provider will conduct a Security Threat Risk Assessment in respect of the STMS Calgary Data Centre in accordance with Schedule 24 (*Privacy Obligations*) of the Agreement within thirty days of the STMS Data Centre Availability Date for the STMS Calgary Data Centre.

5.3.4 STMS Calgary Data Centre Requirements Verification

The Service Provider will complete the Data Centre Requirements Verification described in Section 5.4 of the Data Centre Services SOW of the Agreement to verify that the STMS Calgary Data Centre meets the data centre infrastructure requirements described in Appendix G (*Data Centre Requirements*) of the Data Centre Services SOW. The Data Centre Requirements Verification in respect of the STMS Calgary Data Centre will be completed in accordance with the schedule described in the Transformation Plan.

5.3.5 Provision of Services

The Service Provider will prepare the Customer Environment for Managed Services to enable the Service Provider to provide the Managed Services as described in Section 6 (*Network LAN/WAN*), Section 9 (*Server Systems Management Transformation*), and Section 12 (*Storage and Backup*) of this SOW.

The Service Provider will provide Services from the STMS Calgary Data Centre to the Province as follows:

(a) as Applications (and their associated data) are migrated to the STMS Calgary Data Centre in accordance with Section 15 (*Virtualization and Migration Project*) of this SOW;

(b)

(c) in response to the Service Request process described in the Service Management SOW.

5.4 Reporting and Transformation Credits

5.4.1 Construction Reviews

The WTS Hosting Alliance Management Office Lead and the Service Provider Data Centre Lead (the "**Designated Leads**") will meet to review the construction reporting provided by the Service Provider in respect of each STMS Data Centre as follows:

- the Designated Leads will meet monthly, commencing six months prior to the applicable STMS Data Centre Availability Date, to review the construction reporting; and
- the Designated Leads will meet twice each month, commencing three months prior to the applicable STMS Data Centre Availability Date, to review the construction reporting.

Promptly following each such construction review meeting of the Designated Leads, the Designated Leads will hold update meetings to review the progress on construction of the STMS Data Centre to which the Province and all Other Customers will be invited.

If at any time the actual progress of construction of an STMS Data Centre has significantly fallen behind schedule or the Province is of the opinion that the actual progress of the construction has significantly fallen behind schedule or that an STMS Data Centre will not be completed by the applicable STMS Data Centre Availability Date, the Service Provider will be required:

(a) within fifteen Business Days of receipt of notice from the Province, to produce and deliver to the Province:

(i) a report identifying the reasons for the delay; and

(ii) a plan showing the steps that are to be taken by the Service Provider to complete such STMS Data Centre by the applicable STMS Data Centre Availability Date (the "**Preemptive Remedial Plan**"); and

(b) to work diligently to bring completion of such STMS Data Centre back on schedule in accordance with the Preemptive Remedial Plan approved by the Province.

The Service Provider will notify the Province if, at any time, the actual progress of the construction of an STMS Data Centre is significantly ahead of schedule.

5.4.2 STMS Data Centre Delay

Commencing three months prior to the STMS Data Centre Availability Date for an STMS Data Centre and continuing until the construction of the STMS Data Centre is completed in

accordance with this SOW, if the construction reporting provided in respect of the construction of the STMS Data Centre indicates that the construction of the STMS Data Centre is behind schedule, then:

(a) the Designated Representatives will meet weekly to review the status of the construction against the timelines;

(b) the Service Provider will review the construction of the STMS Data Centre with the Data Centre Services Subcontractor prior to each weekly meeting and will report to the Province on the measures that are being implemented in response to the construction delays; and

(c) the Province and the Service Provider will cooperate to identify any actions that may be taken by any of them in response to the construction delays at the STMS Data Centre and, as they deem appropriate, in investigating alternate sources of data centre capacity.

Promptly following each such construction review meeting of the Designated Leads relating to a delay in construction, the Designated Leads will hold update meetings to review the delays in construction to which the Province and all Other Customers of the STMS Data Centre will be invited.

If the delay in construction of the STMS Data Centre is, at any time determined to be, one month or more, then the Parties will immediately escalate the issue of the construction delays to the Joint Executive Committee under the Agreement. The Province and the Service Provider will continue to review the delay in construction at Joint Executive Committee meetings on a bi-weekly basis until such time as the delays in construction have been eliminated and the construction of the STMS Data Centre is back on schedule.

If either STMS Data Centre is not complete on or before the STMS Data Centre Availability Date for such STMS Data Centre, then the Service Provider shall:

(i) immediately provide the Province with a reasonable plan and schedule (the "**Remedial Plan**") to mitigate the effect of such delay, which schedule shall specify in reasonable detail the manner in, and the latest date by which, such delay is proposed to be mitigated and the applicable STMS Data Centre will be available; and

(ii) thereafter, perform its obligations to achieve all elements of the Remedial Plan in accordance with its terms within the time for the performance of its obligations thereunder.

The Remedial Plan shall also identify options available to respond to the construction delays. The options documented by the Service Provider may include: (i) interim measures in respect of the space currently being used by the Province or Other Customers; (ii) a different delivery site or sites able to respond to the operational requirements of the Province and Other Customers; or (iii) such other measures as the Service Provider is able to identify. The Province shall not be

required to accept any option proposed by the Service Provider and shall accept one of the options proposed by the Service Provider only if it is acceptable to the Province.

If the Service Provider fails to put forward the Remedial Plan, or the delay is not remedied within the requisite period, or the Service Provider puts forward a Remedial Plan and fails to perform its obligations thereunder necessary to achieve all elements of the Remedial Plan in accordance with its terms within the requisite time, or the Province does not accept any of the options proposed by the Service Provider in the Remedial Plan, then in each such case the matter will be escalated to the Joint Executive Committee under the Agreement in accordance with its Governance Process.

5.4.3 Transformation Credits

In the event the Service Provider fails to complete either STMS Data Centre in accordance with this SOW, then the Service Provider will pay the following Transformation Credits to the Province:

- Monthly Out-of-Pocket Assistance;
- VA Future Credits; and
- Data Centre Delay Credits

(collectively, the "**Transformation Credits**").

(a) Monthly Out-of-Pocket Assistance

For each month or any part thereof, that completion of an STMS Data Centre is delayed beyond the applicable STMS Data Centre Availability Date, the Service Provider will reimburse the Province for out-of-pocket expenses incurred in such month as a result of the unavailability of the STMS Data Centre (the "**Monthly Out-of-Pocket Assistance**"), up to the aggregate maximum amount in respect of such STMS Data Centre and month of delay as is set out in Table 2 – Monthly Out-of-Pocket Assistance Cap below. The Province will provide the Service Provider with evidence of the out-of-pocket expenses incurred by it for which the Service Provider is to reimburse the Province, and the Service Provider will pay the Monthly Out-of-Pocket Assistance amounts to the Province within ten Business Days of receipt of such evidence.

For the purposes of Section 5.4.3 (*Transformation Credits*), "out-of-pocket expenses" includes any costs, expenses or other amounts paid to a third party.

Table 2 – Monthly Out-of-Pocket Assistance Cap

Month of Delay beyond STMS Data Centre Availability Date	STMS Calgary Data Centre	STMS Interior Data Centre
> or = 0 months	0	0

> or = 1 month	10,000	$75,000
> or = 2 months	20,000	$100,000
> or = 3 months	20,000	$100,000
> or = 4 months	20,000	$100,000
> or = 5 months	20,000	$100,000
> or = 6 months	0 (see Data Centre Delay Credits, below)	0 (see Data Centre Delay Credits, below)
> or = 7 months	20,000	$100,000
> or = 8 months	20,000	$100,000

For example, if the STMS Interior Data Centre is not completed within four months of the applicable STMS Data Centre Availability Date, then the Service Provider shall reimburse the Province in respect of the following:

(i) for the failure to complete the STMS Interior Data Centre within one month of the applicable STMS Data Centre Availability Date, the Service Provider shall not be required to reimburse the Province for out-of-pocket expenses incurred by the Province in the first month i.e., the aggregate maximum amount will be $0;

(ii) the failure to complete the STMS Interior Data Centre within two months of the applicable STMS Data Centre Availability Date, the Monthly Out-of-Pocket Assistance in respect of out-of-pocket expenses incurred by the Province in the second month, to an aggregate maximum amount in respect of the second month of $75,000;

(iii) the failure to complete the STMS Interior Data Centre within three months of the applicable STMS Data Centre Availability Date, the Monthly Out-of-Pocket Assistance in respect of out-of-pocket expenses incurred by the Province in the third month, to an aggregate maximum amount in respect of the third month of $100,000;

(iv) the failure to complete the STMS Interior Data Centre within four months of the applicable STMS Data Centre Availability Date, the Monthly Out-of-Pocket Assistance in respect of out-of-pocket expenses incurred by the Province in the fourth month up to an aggregate maximum amount of $100,000.

(b) VA Future Credits

For each month that completion of an STMS Data Centre is delayed beyond the applicable STMS Data Centre Availability Date, then the Service Provider will provide the Province with a credit percentage (a "**VA Future Credit Percentage**") that will be used to calculate a credit against future VA Fees (the "**VA Future Credit**"). The amount of the VA Future Credit will be determined based on the VA Future Credit Percentages set out in Table 3 – VA Future Credit Calculation and Table 4 – VA Future Credit Percentage, below. The VA Future Credits will be calculated, in each month following the completion of the STMS Data Centre in respect of which a VA Future Credit Percentage was provided, as follows:

Table 3 – VA Future Credit Calculation

VA Future Credit for month following completion of STMS Data Centre	=	VA Fees for month following completion of STMS Data Centre	X	VA Future Credit Percentage identified in Table 4 – VA Future Credit Percentage, below, for month of delay that is the month following completion of the STMS Data Centre

The Service Provider will calculate the VA Future Credits for the month to which they apply and will provide the Province with a credit in respect of such amount on the monthly invoice, which credit will be set-off against Fees in accordance with Section 15.5 (*Right of Set-Off*) of the Agreement.

The VA Future Credit Percentages must be used in the order in which they were obtained.

The availability of any VA Future Credits in any month shall not prevent the Province from claiming or obtaining any Service Level Credits in any such month to which it may be entitled under Schedule 11 (*Service Levels*).

Table 4 – VA Future Credit Percentage

Month of Delay beyond STMS Data Centre Availability Date	**STMS Calgary Data Centre VA Future Credit**	**STMS Interior Data Centre VA Future Credit**
> or = 0 months	0%	0%
> or = 1 month	0%	0%
> or = 2 months	0%	0%

Month of Delay beyond STMS Data Centre Availability Date	STMS Calgary Data Centre VA Future Credit	STMS Interior Data Centre VA Future Credit
> or = 3 months	0%	0%
> or = 4 months)	20%	10%
> or = 5 months	30%	20%
> or = 6 months	40%	30%
> or = 7 months	50%	40%
> or = 8 months	50%	50%
>9 months	50%	50%

For example, assume completion of the STMS Interior Data Centre is delayed by four months, then the Province is entitled to a VA Future Credit based on the VA Future Credit Percentage identified in Table 4 – VA Future Credit Percentage above for month 4 for the STMS Interior Data Centre (10%). This VA Future Credit will be applied against the Province's VA charges for the fifth month following commencement of Services by the Service Provider. The VA Future Credit for the Province for such month will be the product of the VA Future Credit Percentage (10%) and the Province's VA Fees for such month.

(c) Data Centre Delay Credits

If the completion of an STMS Data Centre is delayed beyond the applicable STMS Data Centre Availability Date by six months, then the Service Provider will pay to the Province a Data Centre Delay Credit in the amount set out in Table 5 – Data Centre Delay Credits below, which Data Centre Delay Credit shall be payable to the Province by the Service Provider as follows:

Table 5 – Data Centre Delay Credits

STMS Calgary Data Centre Data Centre Delay Credit	STMS Interior Data Centre Data Centre Delay Credit
100,000	$250,000

For example, if the STMS Interior Data Centre is delayed by six months, then the Service Provider will pay to the Province the sum of $250,000. The Province may invoice the Service Provider for the Data Centre Delay Credit in respect of the STMS Interior Data Centre at such time as completion of the STMS Interior Data Centre is delayed beyond the applicable STMS

Data Centre Availability Date by six months and the Service Provider will pay the Data Centre Delay Credit to the Province within ten Business Days receipt of the invoice therefor.

In the event the Province elects not to terminate the Agreement under Section 5.4.3(d), then the Service Provider will continue to pay the following Transformation Credits to the Province:

(i) Monthly Out-of-Pocket Assistance; and

(ii) VA Future Credits until construction of the delayed STMS Data Centre has been completed in accordance with this SOW.

(d) Termination

If the completion of an STMS Data Centre is delayed beyond the applicable STMS Data Centre Availability Date by a period of six months (the "**Build Delay Period**"), then the Service Provider will provide the Province, within thirty days after the expiry of the Build Delay Period a report identifying options, in writing, available to the Province, which options may include:

(i) interim measures in respect of the space currently being used by the Province;

(ii) a different delivery site or sites able to respond to the operational requirements of the Province; and

(iii) such other measures as the Service Provider is able to identify at the time, provided that the Province shall have no obligation to accept any option proposed by the Service Provider.

If the Province does not accept any of the options proposed by the Service Provider in its report, then, in addition to the Transformation Credits set forth above (Sections 5.4.3(a) (*Monthly Out-of Pocket Assistance*), Section 5.4.3(b) (*VA Future Credits*) and Section 5.4.3(c) (*Data Centre Delay Credits*), the Province may, without limiting its other rights or remedies, and without cost, charge or liability, immediately terminate the Agreement for Service Provider Material Breach, in which case the provisions of Column 5 entitled "Termination by Province for Service Provider Material Breach" of Schedule 38 (*Fees*) shall apply.

For greater certainty, the Transformation Credits set forth in Section 5.4.3(a) (*Monthly Out-of Pocket Assistance*) and Section 5.4.3(b) (*VA Future Credits*) will continue to apply until the first to occur of: (i) the delayed STMS Data Centre is completed; (ii) the Province elects an option proposed by the Service Provider under Section 5.4.3(d) (*Termination*) that does not include Transformation Credits or otherwise amends the Transformation Credits; or (iii) the Province terminates the Agreement in accordance with Section 5.4.3(d) (*Termination*).

(e) Agreement re Remedies

The Province and Service Provider acknowledge and agree that:

(i) the Service Provider will pay

(A) the Monthly Out-of-Pocket Assistance in 5.4.3(a) in respect of delays in the completion of an STMS Data Centre, unless and until the first to occur of: (1) the completion of the STMS Data Centre; (2) the Province elects an option proposed by the Service Provider under Section 5.4.3(d) that does not include such Transformation Credits or otherwise amends the Transformation Credits; or (3) the Province terminates the Agreement in accordance with Section 5.4.3(d);

(B) the VA Future Credits in Section 5.4.3(b) in respect of delays in the completion of an STMS Data Centre, unless and until the earlier of: (1) the completion of the STMS Data Centre (at which point the right to accumulate further VA Future Credits expires but the obligation of the Service Provider to pay accumulated VA Future Credits survives) ; (2) the Province elects an option proposed by the Service Provider under Section 5.4.3(d) that does not include such Transformation Credits or otherwise amends such Transformation Credits; or (3) the Province terminates the Agreement in accordance with Section 5.4.3(d);

(C) the Data Centre Delay Credits in respect of delays in the completion of the STMS Data Centre, unless and until the Province elects an option proposed by the Service Provider under Section 5.4.3(d) that does not include such Transformation Credits or otherwise amends such Transformation Credits;

(ii) until such time as the Province terminates the Agreement in accordance with Section 5.4.3(d), the Province will not bring any Claims in respect of delays in the completion of the STMS Data Centre other than for payment of the Transformation Credits set out in Sections 5.4.3(a) - 5.4.3(c);

(iii) if the Province terminates the Agreement under Section 5.4.3(d), the termination provisions of the Agreement will apply and the Province shall be entitled to such remedies as are available to it under the Agreement (for greater certainty, termination of the Agreement pursuant to Section 5.4.3(d) is in addition to the obligations of the Service Provider to pay the Transformation Credits prior to termination of the Agreement); and

(iv) if the STMS Data Centre is completed and the Province does not terminate the Agreement under Section 5.4.3(d), then except as provided in Sections 5.4.3(a) - 5.4.3(c), the Service Provider will have no obligation or liability to and no Claims shall be made by the Province in respect of delays in the completion of the STMS Data Centre.

6. NETWORK LAN/WAN

Pursuant to the Network LAN/WAN Transformation Project, the Service Provider will:

(a) provide data communications between the Service Provider Support Locations and the Hosting Locations, enabling remote management and support of the Managed Equipment; and

(b) provide data communications between the Province Network and the STMS Data Centres, enabling the Province to utilize the Managed Equipment located at the STMS Data Centres.

Network LAN/WAN Transformation Project activities have been grouped under three headings:

- Management Network;
- STMS Calgary Data Centre Networking; and
- STMS Interior Data Centre Networking.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Network LAN/WAN Transformation	**Management Network**	Early Circuit Install	See Schedule 23 (*Fees*), Appendix I	Month 0, March, 2009	**Installed and fully operational**
		Design	See Schedule 23 (*Fees*), Appendix I	Month 1, April, 2009	
		Order	See Schedule 23 (*Fees*), Appendix I	Month 2, May, 2009	
		Install	See Schedule 23 (*Fees*), Appendix I	Month 4, July 2009	
		Test and Activate	See Schedule 23 (*Fees*), Appendix I	Month 4, July 2009	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
	STMS Calgary Data Centre Networking	High Level Design	See Schedule 23 (*Fees*), Appendix I	Month 1, April, 2009	**Installed and fully operational**
		STMS Calgary Data Centre Design	See Schedule 23 (*Fees*), Appendix I	Month 3, June 2009	
		Pre Configuration of LAN & WAN Equipment	See Schedule 23 (*Fees*), Appendix I	Month 7, October 2009	
		Installation of Production Network	See Schedule 23 (*Fees*), Appendix I	Month 8, November, 2009	
		LAN & WAN Testing	See Schedule 23 (*Fees*), Appendix I	Month 9, December 2009	
	STMS Interior Data Centre Networking	STMS Interior Data Centre Design	See Schedule 23 (*Fees*), Appendix I	Month 20, November, 2010	**Installed and operational**
		Pre Configuration of LAN & WAN Equipment	See Schedule 23 (*Fees*), Appendix I	Month 24, March 2011	
		Installation of Production Network	See Schedule 23 (*Fees*), Appendix I	Month 25, April, 2011	
		LAN & WAN Testing	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	

6.2 Management Network

The Service Provider will establish network connectivity (the "**Management Network**") to enable the Service Provider to remotely manage the Managed Equipment. The network connectivity to be established is between the Service Provider Support Locations and two connection points to the Province Network at the Province Designated Network Locations. When each STMS Data Centres become available, the Service Provider will also establish Management Network connectivity to each such STMS Data Centre.

While the Management Network will be established in several phases in accordance with the Transformation Plan, there will be an initial, single connection between one Service Provider Support Location and the Province Designated Network Location at S. 15 that will be established by the Hand-Over Date.

6.2.1 Early Circuit Install

6.2.1.1 Service Provider Responsibilities

The Service Provider will:

(a) establish an initial, single connection between one Service Provider Support Location and the Province Designated Network Location S. 15 by the Hand-Over Date;

(b) prepare a detailed design for the initial single connection;

(c) order and install the circuit and hardware;

(d) provide the Province with the Service Provider's access requirements to the Managed Equipment and request that the Province provide the Third Party Gateway;

(e) test connectivity to the Managed Equipment in cooperation with the Province; and

(f) provide written notification to the Province when the Early Circuit Install Milestone (see table above) has been achieved (when the Management Network connectivity is available for use).

6.2.1.2 Province Responsibilities

The Province will:

(a) provide site contacts at the Province Designated Network Location S. 15 S. 15

(b) approve physical access and provide directions for circuit and equipment installation;

(c) prepare, install and configure the Third Party Gateway in cooperation with the Service Provider; and

(d) test connectivity to the Managed Equipment in cooperation with the Service Provider and utilizing the Third Party Gateways.

6.2.2 Design

6.2.2.1 Service Provider Responsibilities

The Service Provider will:

(a) prepare a detailed design for the remaining components of the Management Network;

(b) provide the Province with the Service Provider's access requirements to the Managed Equipment;

(c) create a bill of materials for the network components required to connect the STMS Data Centres to SPAN BC;

(d) conduct peer review of the detailed design;

(e) obtain the approval of the Province to proceed with the installation of the remaining components of the Management Network; and

(f) provide written notification to the Province when the Design Milestone (see table above) has been achieved (when the Province has approved the installation of the remaining components of the Management Network).

6.2.2.2 Province Responsibilities

The Province will:

(a) facilitate the review and approval for the connection of the remaining components of the Management Network to the Province Network and the installation of the Service Provider Network Equipment at Province Designated Network Locations; and

(b) prepare a design for the Third Party Gateways required at Province Designated Network Locations.

6.2.3 Order

The Service Provider will

(a) order the circuits and Service Provider Network Equipment (not including any Third Party Gateways) required to establish the Management Network; and

(b) provide written notification to the Province when the Order Milestone (see table above) has been achieved (when the circuits and the Service Provider Network Equipment have been ordered).

The Province will order Third Party Gateway hardware.

6.2.4 Install

6.2.4.1 Service Provider Responsibilities

The Service Provider will:

(a) install the Management Network circuits at the Province Designated Network Locations;

(b) install Management Network equipment at Service Provider Support Locations and at the Province Designated Network Locations; and

(c) provide written notification to the Province when the Install Milestone (see table above) has been achieved (when the circuits and equipment are installed).

6.2.4.2 Province Responsibilities

The Province will:

(a) provide site contacts at the Province Designated Network Locations;

(b) provide space and power for the Service Provider Management Network equipment at the Province Designated Network Locations;

(c) approve physical access and provide directions for circuit and equipment installation at the Province Designated Network Locations;

(d) prepare, install and configure the Third Party Gateway in cooperation with the Service Provider; and

(e) support the Service Provider's installation of equipment at the Province Designated Network Locations.

6.2.5 Test and Activate

The Service Provider will:

(a) test connectivity to the Managed Equipment in cooperation with the Province;

(b) following successful completion of Management Network connectivity testing, activate the Management Network connectivity in accordance with the Change Management Process as described in the Service Management SOW;

(c) provide written notification to the Province when the Test and Activate Milestone (see table above) has been achieved (following successful completion of the Management Network connectivity testing and activation of the Management Network); and

(d) operate the Management Network in accordance with the Data Centre Services SOW and the Service Management SOW.

The Province will test connectivity to the Managed Equipment in cooperation with the Service Provider and utilizing the Third Party Gateways.

6.2.6 Completion

For the purposes of this SOW, the Management Network Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 6.2 (*Management Network*) have been achieved.

6.3 STMS Calgary Data Centre Networking

The Service Provider will:

(a) establish a network at the STMS Calgary Data Centre to enable it to provide the Managed Services and to connect to the Province Network; and

(b) establish network connectivity between the STMS Calgary Data Centre and the two Province Designated Network Locations, enabling Clients to utilize the Managed Equipment located at the STMS Calgary Data Centre.

6.3.2 High Level Design

The Service Provider and the Province will review and confirm the high level design for the Network connecting the STMS Data Centres and two Province Designated Network Locations as described in the Network section of the Data Centre Services SOW. Any changes to the high level design will be implemented in accordance with the Change Management Process described in the Service Management SOW.

The Service Provider will provide written notification to the Province when the High Level Design Milestone (see table above) has been achieved (when the Service Provider and the Province have reviewed and confirmed the high level design for the Network connecting the STMS Data Centres and two Province Designated Network Locations as described in the Network section of the Data Centre Services SOW).

6.3.3 STMS Calgary Data Centre Design

The Service Provider will:

(a) develop a design for the network components that are internal to the STMS Calgary Data Centre;

(b) review its design for the network components that are internal to the STMS Calgary Data Centre with the Province; and

(c) provide written notification to the Province that the Calgary Data Centre Design Milestone (see table above) has been achieved (when the design is complete and the Province has reviewed the design for the network components that are internal to the STMS Calgary Data Centre).

The Province will review the design for the network components that are internal to the STMS Calgary Data Centre.

6.3.4 Pre-Configuration of LAN & WAN Equipment

The Service Provider will:

(a) take delivery, at an alternate Service Provider Support Location, of the equipment necessary to establish the internal network at the STMS Calgary Data Centre prior to the availability of the STMS Calgary Data Centre;

(b) configure such equipment at the alternate Service Provider Support Location;

(c) ship configured equipment to the STMS Calgary Data Centre; and

(d) provide written notification to the Province when the Pre-Configuration of LAN & WAN Equipment Milestone (see table above) has been achieved (when the configured equipment has arrived at the STMS Calgary Data Centre).

6.3.5 Installation of Production Network

6.3.5.1 Service Provider Responsibilities

The Service Provider will:

(a) install the circuits connecting the STMS Calgary Data Centre to the Province Designated Network Locations;

(b) install network equipment at the STMS Calgary Data Centre. The network equipment at the STMS Calgary Data Centre connects the Managed Equipment at the STMS Data Centre; and

(c) provide written notification to the Province when the Installation of Production Network Milestone (see table above) has been achieved (when the circuits and equipment are installed).

6.3.5.2 Province Responsibilities

The Province will:

(a) Order and retain cost-responsibility for the circuits connecting the STMS Calgary Data Centre to the Province Designated Network Locations;

(b) provide site contacts at Province Designated Network Locations;

(c) provide space and power for the Service Provider Network equipment at the Province Designated Network Locations;

(d) approve physical access and provide directions for circuit installation; and

(e) configure the Third Party Gateway to enable the Clients to access the Managed Equipment located at the STMS Calgary Data Centre.

6.3.6 LAN & WAN Testing

The Service Provider will:

(a) test connectivity to the Managed Equipment in cooperation with the Province;

(b) following successful completion of connectivity testing, activate the network connectivity in accordance with the Change Management Process described in the Service Management SOW (if the connectivity testing is not successfully completed, then the Service Provider will continue to rectify the connectivity to the Managed Equipment until the connectivity testing is successfully completed); and

(c) provide written notification to the Province when the LAN & WAN Testing Milestone (see table above) has been achieved (when the network connecting the STMS Calgary Data Centre to the Province Network is active).

The Province will test connectivity to the Managed Equipment in cooperation with the Service Provider and utilizing the Third Party Gateway.

6.3.7 Completion

For the purposes of this SOW, the STMS Calgary Data Centre Networking Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 6.3 (*STMS Calgary Data Centre Networking*) have been achieved.

6.4 STMS Interior Data Centre Networking

The Service Provider will:

(a) establish a network at the STMS Interior Data Centre to enable it to provide the Managed Services and to connect to the Province Network at a single Province Designated Network Location;

(b) establish redundant network connectivity between the STMS Interior Data Centre and the STMS Calgary Data Centre; and

(c) eliminate one of the two network connections between the STMS Calgary Data Centre and the Province Designated Network Locations such that the STMS Calgary Data Centre will remain connected to one Province Designated Location

and the STMS Interior Data Centre will be connected to the other Province Designated Network Location.

6.4.2 STMS Interior Data Centre Design

The Service Provider will:

(a) develop a design for the network components that are internal to the STMS Interior Data Centre;

(b) review its design for the network components that are internal to the STMS Interior Data Centre with the Province; and

(c) provide written notification to the Province when the STMS Interior Data Centre Design Milestone (see table above) has been achieved (when the design is complete and the Province has reviewed the design for the network components that are internal to the STMS Interior Data Centre).

The Province will review the design for the network components that are internal to the STMS Interior Data Centre.

6.4.3 Pre-Configuration of LAN & WAN Equipment

The Service Provider will:

(a) take delivery, at an alternate Service Provider Support Location, of the equipment necessary to establish the internal network at the STMS Interior Data Centre prior to the availability of the STMS Interior Data Centre;

(b) configure such equipment at the alternate Service Provider Support Location;

(c) ship configured equipment to the STMS Interior Data Centre; and

(d) provide written notification to the Province when the Pre-Configuration of LAN & WAN Equipment Milestone (see table above) has been achieved (when the configured equipment has arrived at the STMS Interior Data Centre).

6.4.4 Installation of Production Network

6.4.4.1 Service Provider Responsibilities

The Service Provider will:

(a) install the circuit connecting the STMS Interior Data Centre to the Province Designated Network Location;

(b) install the circuits connecting the STMS Interior Data Centre to the STMS Calgary Data Centre;

(c) remove one of the circuits connecting the STMS Calgary Data Centre to the Province Designated Network Locations;

(d) install network equipment at the STMS Interior Data Centre. The network equipment at the STMS Interior Data Centre connects the Managed Equipment at the STMS Data Centre; and

(e) provide written notification to the Province when the Installation of Production Network Milestone (see table above) has been achieved (when the circuits and equipment are installed).

6.4.4.2 Province Responsibilities

The Province will:

(a) order and retain cost-responsibility for the circuit connecting the STMS Interior Data Centre to the Province Designated Network Location;

(b) order and retain cost-responsibility for the circuits connecting the STMS Interior Data Centre to the STMS Calgary Data Centre;

(c) provide site contacts at Province Designated Network Locations;

(d) provide space and power for the Service Provider Network equipment at the Province Designated Network Locations;

(e) approve physical access and provide directions for circuit installation and decommissioning; and

(f) configure the Third Party Gateway to enable the Clients to access the Managed Equipment located at the STMS Interior Data Centre.

6.4.5 LAN & WAN Testing

The Service Provider will:

(a) test connectivity to the Managed Equipment in cooperation with the Province;

(b) following successful completion of connectivity testing, activate the network connectivity in accordance with the Change Management Process described in the Service Management SOW; and

(c) provide written notification to the Province when the LAN & WAN Testing Milestone (see table above) has been achieved (when the network connecting the STMS Interior Data Centre to the Province Network is active and the network connecting the STMS Interior Data Centre and the STMS Calgary Data Centre is active).

The Province will test connectivity to the in scope devices in cooperation with the Service Provider and utilizing the Third Party Gateways.

6.4.6 Completion

For the purposes of this SOW, the STMS Interior Data Centre Networking Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 6.4 (*STMS Interior Data Centre Networking*) have been achieved.

7. SERVICE MANAGEMENT

Service Management comprises the processes and tools for performance of:

(a) incident management;

(b) change management;

(c) problem management;

(d) request management;

(e) asset management;

(f) billing; and

(g) reporting; and

The purpose of the Service Management Transformation Project is to establish the Service Provider Service Desk Tool, establish Service Management processes, integrate with Province Service Desk Tool, implement a Billing Module and establish a Reporting Portal.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Service Management Transformation	**Establish Service Provider Service Desk Tool and Processes**	Process Integration Workshops	See Schedule 23 (*Fees*), Appendix I	Month 2-4 May, 2009, July, 2009	**Service Provider manages the services using integrated service management processes (Service Provider and Province), the**
		DW with Dispatch Interface for Incidents	See Schedule 23 (*Fees*), Appendix I	Month 5, August, 2009	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
		Non-Dispatch Interface from Province Service Management Systems to Service Provider Service Desk Systems for Incident	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	**Service Provider Service Desk Tool, the Dispatch Interface and the Non-Dispatch Interface**
		First Draft of Service Management Section of the Manual	See Schedule 23 (*Fees*), Appendix I	Month 4, July, 2009	**Asset Centre is loaded with Province data and is used to maintain an accurate and timely Province inventory**
		Initial Asset Centre Load	See Schedule 23 (*Fees*), Appendix I	Month 4, July, 2009	
		Asset Inventory Final Reconciliation	See Schedule 23 (*Fees*), Appendix I	Month 5, August, 2009	
		Asset Inventory Reconciliation Reporting	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	
		Service Management Section of the Manual	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	
		Future Mode of Operation (FMO) Training	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	
		Service Provider Service Desk Tool Training	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	
		Go Live	N/A	Month 6, September, 2009	
	Additional Service Provider Service Management Systems	Prepare Billing Module	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	**Service Catalogue unit price billing capability is ready for Month 7**
		Test Billing Function	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	
		Activate Billing Module	N/A	Month 6, September, 2009	
		Develop Reporting Portal	See Schedule 23 (*Fees*), Appendix I	Month 3, June, 2009	**Reporting available online to the Province**
		Reporting Portal in Production	N/A	Month 6, September, 2009	

7.2 Establish Service Provider Service Desk Tool and Processes

The Service Provider will implement, customize, and configure its Service Desk Tool as described in this section.

Further to the phases of the Service Management Transformation Project described in Sections 7.2.1 to 7.2.4 of this SOW, the Service Provider, with the Province's cooperation, will implement the Incident Management, Change Management, Problem Management and Request Management functions of the Service Provider Service Desk Tool and related processes (as described in the Service Management SOW). The Service Provider, with the Province's cooperation, will implement the Asset Management functions of the Service Provider Service Desk Tool and related processes in the phase of the Service Management Transformation Project described in Section 7.2.5 of this SOW.

7.2.1 Process Integration Workshops

The Service Provider will:

(a) facilitate process integration workshops with the Province to identify how to integrate the Service Management processes of the Parties, such workshops to identify the necessary process elements (integration points, data sets, data structures) so that the configuration of the processes and tools can be completed as described in this section; and

(b) provide written notification to the Province when the Process Integration Workshops Milestone (see table above) has been achieved (when the process integration workshops have been held, the necessary process elements have been identified and the Province has participated in the workshops).

The Province will participate in the process integration workshops as reasonably scheduled by the Service Provider.

7.2.2 DW with Dispatch Interface for Incidents

This phase of the Service Management Transformation Project relates to the dispatch interface for Incidents (the "**Dispatch Interface**") between the Province Service Desk Tool and the Service Provider Service Desk Tool. The Dispatch Interface will allow the Province's CSC (as defined in the Service Management SOW) to assign Incidents directly to the Service Provider and allow updates from and between the two Service Desk Tools.

7.2.2.1 Service Provider Responsibilities

The Service Provider will:

(a) design and develop the Dispatch Interface in consultation with the Province;

(b) test the Dispatch Interface between the Province Service Management Systems (as defined in the Service Management SOW) and the Service Provider Service Desk Tool by:

(i) working with the Province to define test cases and acceptance test criteria to test the Dispatch Interface; and

(ii) conducting the unit, integration and user acceptance testing of the Dispatch Interface with the Province so as to meet the agreed to acceptance test criteria;

(c) develop a process for immediate notification to the Province of Priority 1 and 2 Incidents that are detected by the Service Provider's auto-generated Incident process; and

(d) provide written notification to the Province when the Service Provider Service Desk Tool with Dispatch Interface for Incidents Milestone (see table above) has been achieved (when the Province's CSC can assign Incidents directly to the Service Provider and allow updates from and between the two Service Desk Tools).

7.2.2.2 Province Responsibilities

The Province will:

(a) design, develop, and integrate changes to Province systems including the Province Service Desk Tool to support the Service Provider's design and development activities for the Dispatch Interface in consultation with the Service Provider;

(b) work with the Service Provider to:

(i) complete common data format templates;

(ii) complete interface format templates; and

(iii) define test cases and acceptance test criteria to test the Dispatch Interface;

(c) participate in the testing of the Dispatch Interface conducted by the Service Provider to meet the agreed to acceptance test criteria; and

(d) develop a process to receive notification of Priority 1 and 2 Incidents that are detected by the Service Provider's auto-generated Incident process and enter them into the Province Service Desk Tool.

7.2.3 Non-Dispatch Interface from Province Service Management Systems to Service Provider Management Tool for Incident

The Service Provider Service Desk Tool supports auto-generation of Incident tickets as a result of operations events that are reported to it by the Service Provider's service operations tools. Therefore, the Service Provider Service Desk Tool will contain Incident information that has not been recorded in the Province Service Desk Tool. The non-dispatch interface for Incidents (the "**Non-Dispatch Interface**") will update the Province Service Desk Tool each day with all auto-generated tickets for Minor Incidents (as defined in the Service Management SOW) in the Service Provider Service Desk Tool that have not been recorded in the Province Service Desk Tool and that have not otherwise been sent to the Province Service Desk Tool in the previous batch process. The intent is to ensure that the monthly reporting that the Service Provider generates from the Service Provider Service Desk Tool remains consistent with the Province Service Desk Tool system of record for Incidents, other than Excluded Minor Incidents (as defined in Section 1.11.5 of the Service Management SOW).

7.2.3.1 Service Provider Responsibilities

The Service Provider will:

(a) design and develop the Non-Dispatch Interface that:

(i) creates an extract that identifies the auto-generated Minor Incidents (other than Excluded Minor Incidents) that have not been entered, but are required to be entered, into the Province Service Desk Tool;

(ii) submits the extract to the Province Service Management Systems for updating into the Province Service Desk Tool; and

(iii) verifies on a monthly basis that the Province Service Desk Tool and the Service Provider Service Desk Tool are synchronized with respect to Incidents, other than Excluded Minor Incidents;

(b) test the Non-Dispatch Interface between the Province Service Management Systems and the Service Provider Service Desk Tool by, for example:

(i) working with the Province to define test cases and acceptance test criteria to test the Non-Dispatch Interface; and

(ii) conducting the unit, integration and user acceptance tests of the Non-Dispatch Interface with the Province's participation including verification of the synchronization process as well as the remediation of deficiencies so as to meet the agreed to acceptance test criteria; and

(c) provide written notification to the Province when the Non-Dispatch Interface from Province Service Management Systems to Service Provider Service Desk Tool for Incident Milestone (see table above) has been achieved (when the Province Service Management Systems including the Province Service Desk Tool

can accept the extract that identifies the auto-generated Minor Incidents, other than the Excluded Minor Incidents, that are required to be entered into the Province Service Management Systems).

7.2.3.2 Province Responsibilities

The Province will:

(a) in connection with the Service Provider's design and development of the Non-Dispatch Interface:

(i) design, develop, modify and integrate changes to the Province Service Management Systems including the Province Service Desk Tool to accept the extract that identifies the auto-generated Minor Incidents (other than the Excluded Minor Incidents) that are required to be entered into the Province Service Management Systems; and

(ii) support the Service Provider's design and development activities for the Non-Dispatch Interface; and

(b) participate in the unit, integration, and user acceptance testing of the Non-Dispatch Interface by:

(i) performing testing for all Province Service Management Systems including remediation of deficiencies; and

(ii) verifying the results of user acceptance testing on the Non-Dispatch Interface.

7.2.4 Service Management Section of the Manual

The Service Provider will develop the Service Management Section of the Manual in accordance with the requirements for the Manual in the Agreement and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*) and it will describe Change Management, Incident Management, Problem Management, Asset Management, and Request Management processes (as defined in the Service Management SOW), as refined in the process integration workshops.

7.2.4.1 First Draft of Service Management Section of the Manual

The Service Provider will:

(a) complete the first draft of the Service Management section of the Manual in accordance with the requirements for the Manual in the Agreement and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*); and

(b) provide written notification to the Province when the First Draft of Service Management Section of the Manual Milestone (see table above) has been

achieved (when the Province has reviewed the draft and provided feedback and verification).

The Province will review the draft and provide feedback and verification.

7.2.4.2 Final Draft of Service Management Section of the Manual

The Service Provider will:

(a) in accordance with the Agreement, finalize and submit the Service Management section of the Manual to the Province in accordance with the requirements for the Manual in the Agreement; and

(b) provide written notification to the Province when the Service Management Section of the Manual Milestone (see table above) has been achieved (when the Service Provider has finalized and submitted it to the Province).

7.2.5 Asset Centre Module

Asset Centre is a module within the Service Provider Service Desk Tool that maintains the inventory of the Managed Equipment and Software managed by the Service Provider as part of the Managed Services. The Parties will use the Asset Centre to support the volumetric based billing.

7.2.5.1 Initial Asset Centre Load

The Province will provide to the Service Provider an inventory of the Managed Equipment and Software assets to be managed by the Service Provider as part of the Services within 10 Business Days of the Hand-Over Date. The Service Provider and the Province will work together to perform preliminary reconciliation of the inventory list as follows:

(a) the Service Provider will identify missing information and data in the inventory provided by the Province; and

(b) the Province will provide the missing information and data if available.

The Province and the Service Provider will work together to categorize the inventory into the billing units described in the Service Catalogue.

When these steps have been completed, the Service Provider will load the inventory into the Asset Centre.

The Service Provider will provide written notification to the Province when the Initial Asset Centre Load Milestone (see table above) has been achieved (when the initial asset inventory has been reconciled, categorized into billing units and loaded into the Asset Centre).

7.2.5.2 Asset Inventory Final Reconciliation

The Service Provider will perform a further reconciliation of the inventory initially loaded into the Asset Centre with the inventory discovered by the Service Provider's service operation tools.

The Parties will review and agree as to any discrepancies between the data initially loaded into the Asset Centre and the inventory identified by the Service Provider's service operation tools prior to updating the Asset Centre.

The Service Provider will provide written notification to the Province when the Asset Inventory Final Reconciliation Milestone (see table above) has been achieved (when the asset inventory has been further reconciled and the Service Provider and the Province have reviewed and agreed on the final reconciliation).

7.2.5.3 Asset Inventory Reconciliation Reporting

The asset inventory reconciliation report is intended to support the Province's reconciliation of the assets related to the Services and the assets the Province charges to the Clients through the Province Ordering System.

The Service Provider will design and develop the asset reconciliation report in consultation with the Province.

The Province will provide requirements for the asset reconciliation report.

The Service Provider will provide written notification to the Province that the Asset Inventory Reconciliation Reporting Milestone (see table above) has been achieved (when it has designed and developed the asset reconciliation report, in consultation with the Province).

7.2.6 Training

The Service Provider will develop and conduct training for Province and Service Provider employees as described in this section.

7.2.6.1 Future Mode of Operation (FMO) Training

The Service Provider will:

(a) develop training for Service Provider Personnel and Province Staff relating to the Service Management processes described in the Service Management section of the Manual, such training to be targeted to the specific requirements of the Service Provider Personnel and the Province Staff with a view to educating them about the functions and operations of the new processes; and

(b) provide written notification to the Province when the Future Mode of Operations (FMO) Training Milestone (see table above) has been achieved (when Service Provider Personnel and Province Staff have participated in the training sessions organized by the Service Provider).

The Province will identify Province Staff and facilitate the participation of such Province Staff in the training organized by the Service Provider.

7.2.6.2 Service Provider Service Desk Tool Training

The Service Provider will:

(a) develop training in the use of its Service Desk Tool for appropriate Province Staff, such training to focus on the functions and operations of the Service Provider Service Desk Tool to enable such Province Staff to use the tool in the performance of their responsibilities; and

(b) provide written notification to the Province when the Service Provider Service Desk Tool Training Milestone (see table above) has been achieved (when appropriate Province Staff have participated in the training organized by the Service Provider).

The Province will identify Province Staff and facilitate the participation of such Province Staff in the training organized by the Service Provider.

7.2.7 Production Readiness

Following the Hand-Over Date, the Province and the Service Provider will cooperate to review the activities described in Sections 7.2.1 (*Process Integration Workshops*) through 7.2.6 (*Training*) of this SOW to determine the extent to which such activities must be completed prior to the Service Provider Service Desk Tool and related Service Provider and Province Service Management Systems being implemented in production.

The Service Provider will notify the Province when:

(a) the activities described in Sections 7.2.1 (*Process Integration Workshops*) through 7.2.6 (*Training*) have been completed to the extent that the Parties agreed such activities needed to be completed prior to the Service Provider Service Desk Tool and related Service Provider and Province Service Management Systems being implemented in production; and

(b) the Service Provider Service Desk Tool, Province Service Desk Tool, Service Provider Service Management Systems and Province Service Management Systems have been integrated and are ready for use in production.

7.2.8 Go Live

Upon the Province's receipt of the notice from the Service Provider referred to in Section 7.2.7 (*Production Readiness*), and with the agreement of the Province and the Service Provider, the Service Provider, with the Province's cooperation, will implement the Service Provider Service Desk Tool, Province Service Desk Tool, Service Provider Service Management Systems and Province Service Management Systems (including the Dispatch Interface and the Non-Dispatch

Interface) in production and thereafter the Parties will use such items in connection with the Services.

7.2.9 Completion

For the purposes of this SOW, the Establish Service Provider Service Desk Tool and Processes Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 7.2 (*Establish Service Provider Service Desk Tool Processes*) have been achieved.

7.3 Additional Service Provider Service Management Systems

In addition to the Service Desk Tool, the Service Provider will implement its Billing Module and a Reporting Portal.

7.3.1 Billing Module

The Service Provider will configure an existing Billing Module to allow the Service Provider to invoice the Province for Services provided in accordance with the Agreement and the Province to pay such invoices in accordance with the Agreement. The Service Provider expects to have the Billing Module operational by Month 7 of the Term of the Agreement. The Service Provider will continue to rely on its manual method of producing invoices until the Billing Module is configured and implemented in production in accordance with Section 7.3.1 (*Billing Module*).

7.3.1.1 Prepare Billing Module

In connection with configuring its Billing Module, the Service Provider will:

(a) identify the sources for the volumetric based billing and other billing data;

(b) define the processes or methods to collect the billing data from the sources identified by the Service Provider;

(c) develop or modify, if necessary, tools to automate the feeds of billing data into the Billing Module; and

(d) develop in consultation with the Province, prototype presentations of the invoices from the Billing Module in response to Province requirements for presentation of the invoices.

The Province will provide to the Service Provider its requirements for presentation of the invoices from the Billing Module in order to support the Province's reconciliation of the Service Provider invoices with: (i) information in the Province Ordering System; and (ii) the Fees for the Services set out in Schedule 23 (*Fees*) of the Agreement.

The Service Provider will provide written notification to the Province when the Prepare Billing Module Milestone (see table above) has been achieved (when the prototype presentations of the invoices from the Billing Module have been developed in consultation with the Province).

7.3.1.2 Test Billing Function

To support the testing of the Billing Module, the Service Provider will work with the Province to define test cases and acceptance test criteria to test the Billing Module and conduct the test of the Billing Module with the Province so as to meet the agreed to acceptance test criteria.

The Province will work with the Service Provider to define test cases and acceptance test criteria to test the Billing Module and participate in the testing of the Billing Module conducted by the Service Provider to meet the agreed to acceptance test criteria.

The Service Provider will provide written notice to the Province that the Test Billing Function Milestone (see table above) has been achieved when the testing of the Billing Module has been completed and the Billing Module is ready for implementation in production.

7.3.1.3 Activate Billing Module

The Service Provider will notify the Province following implementation of the Billing Module in production that it has converted from its interim manual billing process and will thereafter use the Billing Module to prepare invoices.

The Service Provider will provide written notification to the Province when the Activate Billing Module Milestone (see table above) has been achieved (when the Billing Module is implemented in production).

7.3.2 Reporting Portal

The reporting portal is a web-based reporting repository that provides the Province with access to electronic copies of the reports identified in Schedule 21 (*Reporting Requirements*) of the Agreement or in Appendix B of the Statements of Work.

The Service Provider expects to have the reporting portal operational by Month 7 of the Term of the Agreement. The Service Provider will develop a contingency method for report distribution if the reporting portal will not be operational by Month 7.

7.3.2.1 Develop Reporting Portal

The Service Provider will:

(a) develop its web-based reporting portal; and

(b) provide written notification to the Province when the Develop Reporting Portal Milestone (see table above) has been achieved (when the web-based reporting portal has been developed and Province Staff have appropriate levels of access to it).

The Province will provide the Service Provider with details of the levels of access to be granted to Province Staff for access to the web-based reporting portal.

7.3.2.2 Testing

To support the testing of the web-based reporting portal the Service Provider will work with the Province to define test cases and acceptance test criteria to test the web-based reporting portal and conduct the test of the web-based reporting portal with the Province so as to meet the agreed to acceptance test criteria.

The Province will work with the Service Provider to define test cases and acceptance test criteria to test the reporting portal and participate in the testing of the web-based reporting portal conducted by the Service Provider to meet the agreed to acceptance test criteria.

The Service Provider will provide written notice to the Province when the testing of the web-based reporting portal has been completed and the web-based reporting portal is ready for implementation in production.

7.3.2.3 Reporting Portal in Production

The Service Provider will notify the Province that the Reporting Portal in Production Milestone (see table above) has been achieved when it has implemented the web-based reporting portal in production and the Parties will thereafter use the web-based reporting portal for access to reports.

7.3.3 Completion

For the purposes of this SOW, the Additional Service Provider Service Management Systems Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 7.3 (*Additional Service Provider Service Management Systems*) have been achieved.

8. MAINFRAME SERVICES MIGRATION PROJECT

Managed Mainframe Services comprise the stable, secure mainframe computing platform and application production environment operating on the Mainframe System (as defined in the Managed Mainframe Services SOW), which will be provided by the Service Provider to the Province from the in accordance with the Managed Mainframe Services SOW. The Province outsourced the performance of mainframe services to a third party (the "**Current MF Provider**").

The Service Provider shall be responsible for performing the Managed Mainframe Services described in the Managed Mainframe Services SOW upon the date that is the earlier of: (i) completion of the Mainframe Services Migration (as defined below);

The Mainframe Services Migration Project sets forth the provisions regarding the migration the Province's application production environment from the mainframe system being operated by the Current MF Provider to a new hardware and software environment installed by the Service Provider at the (the "**Mainframe Services Migration**"). The transformation project will take place in three phases: (1) the development of an operational assessment (or bridge plan); (2) the development of a detailed migration plan (the "**Detailed**

Migration Plan"); and (3) the performance of the actual mainframe migration in accordance with the Detailed Migration Plan.

The Mainframe Services Migration Transformation Project is described in the following sections below:

- Mainframe Operational Assessment and Plan;
- Detailed Migration Plan;
- Execution of the Detailed Migration Plan; and
- Potential Future Migration Projects.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Mainframe Services Migration	**Mainframe Operational Assessment and Plan**	Mainframe Operational Assessment and Plan	See Schedule 23 (*Fees*), Appendix I	At issue for Inquiry	**Bridge Plan from Current MF Provider to Service Provider**
	Detailed Migration Plan	Detailed Migration Plan	See Schedule 23 (*Fees*), Appendix I		**Detailed plan and time schedule with identified risks and mitigation and back out options**
NTD: The line immediately below and the line immediately below the cell to the right (Execution of the Detailed Migration Plan) should be deleted	**Execution of the Detailed Migration Plan**	Staff Preparation	See Schedule 23 (*Fees*), Appendix I		**Operating documentation and Service Provider trained staff**

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
		Mainframe hardware and swing gear installed at At issue for Inquiry	See Schedule 23 (*Fees*), Appendix I		**New environment procured, installed and tested; ready for migration of Province data**
		Replace exits, usermods, utilities and automation that are not provided by the Province	See Schedule 23 (*Fees*), Appendix I		
		Mainframe hardware installed in DR site	See Schedule 23 (*Fees*), Appendix I		
		Mock 0 Test	See Schedule 23 (*Fees*), Appendix I	At issue for Inquiry	**Migration test passes all test criteria**
		Mock 1 Test	See Schedule 23 (*Fees*), Appendix I		
		Migration	See Schedule 23 (*Fees*), Appendix I		**Migration executed on the planned schedule, with no data loss**
		Tapes shipped from S15 to Calgary	See Schedule 23 (*Fees*), Appendix I		**All tapes transformed**
		Tape Transformation (encryption)	N/A		
		DR Recovery Exercise (Test)	See Schedule 23 (*Fees*), Appendix I	Date to be confirmed during Mainframe Operational Assessment and Plan	**Successful completion against DR test criteria**

8.1 Mainframe Operational Assessment and Plan

The Service Provider will conduct an operational assessment of the mainframe services being provided by the Current MF Provider based on information provided by the Province. Based on such operational assessment the Service Provider and the Province will jointly develop a bridge plan (the "**Bridge Plan**") for the migration of the mainframe services from the Current MF Provider to the Service Provider at the

The Service Provider will prepare and deliver to the Province the Bridge Plan, which shall:

(a) describe the reports, documentation and custom software code that will be provided by the Current MF Provider; identify any reports, documentation and custom software code that need to be developed by the Service Provider; and provide specifications for the reports, documentation and custom software code that will be developed by the Service Provider;

(b) be based on the Service Provider receiving the reports, documentation and custom software code in accordance with Schedule 23 (*Fees*) of the Agreement or as otherwise made available pursuant to the Change Order Process;

(c) have the Service Provider commence performing Managed Mainframe Services including identification of the activities necessary to develop the operational processes and documentation and to provide training to Province Staff and Service Provider Personnel on or before the Managed Mainframe Services Commencement Date (as such defined in the Managed Mainframe Services SOW);

(d) describe any updates to hardware and software configurations defined in the Managed Mainframe Services SOW;

(e) describe any system integration requirements with the Current MF Provider such as data replication (DASD mirroring) including the requirements for the hardware and network connections to the Current MF Provider DASD to support the data migration of the mainframe DASD environment from the Current MF Provider data centre at the Province Data Centre S. 15

(f) describe any transition assistance services required from the Current MF Provider to support Service Provider's assumption of responsibility for the Managed Mainframe Services;

(g) identify in consultation with the Province any Work-in-Progress Projects anticipated to be underway at the time of the Mainframe Services Migration;

(h) describe the Service Provider's testing of the migration of the Managed Mainframe Services that will include:

(i) development of test cases;

(ii) testing the integration of mainframe hardware and software by the Service Provider without the use of Clients' Applications or data (the "**Mock 0 Test**") including the verification of custom software code transferred to the Service Provider or developed by the Service Provider; and

(iii) testing by the Service Provider and the Province of the migration of the mainframe services from the Current MF Provider to the Service Provider (the "**Mock 1 Test**") including Applications (and data of Clients) and user verification of the custom software code and network connectivity; and

(iv) testing for the Fallback Plan;

(i) establishment of the schedule for the exercise of the Disaster Recovery Plan for the Managed Mainframe Services;

At issue for Inquiry

(j) provision for the shipment of all tapes of the Province that are not disaster recovery tapes (the "**Non-DR Tapes**") to the and their transformation to encrypted media (for greater certainty, all tapes of the Province prior to the Managed Mainframe Services Commencement that are disaster recovery tapes (the "**DR Tapes**") will remain the responsibility of the Province);

(k) description of the integration of the Mainframe Services Migration plan and the plan to be developed by the Province for the phase out of the Current MF Provider;

(l) description of any network configuration changes required in support of the Mainframe Services Migration; and

(m) description of the activities necessary for the Mainframe Services Migration at a level of detail sufficient to allow the parties (including, in the case of the Province, Clients) to confirm: (i) the schedule for their participation; and (ii) the commitments with respect to such participation that they are required to make;

8.1.2 Additional Service Provider Responsibilities

The Service Provider will:

(a) receive the reports, documentation and custom software code that will be provided by the Current MF Provider; and receive specifications for the reports, documentation and custom software code that will be developed by the Service Provider;

(b) prepare, in consultation with the Province, an outline for the plan for the Service Provider to commence performing and for the Province to receive the Managed Mainframe Services including identification of the activities necessary to develop the operational processes and documentation and to provide training to the Service Provider Personnel and the Province Staff, as may be applicable;

(c) review with the Province the security resource definitions in place at the Current MF Provider to identify updates required to implement the security resource definitions for the Managed Mainframe Services in the
At issue for Inquiry
in areas that have no direct impact on Clients (for example, as may be required for the Service Provider storage environment or the Service Provider Mainframe System Software);

(d) update the hardware and software configurations described in the Managed Mainframe Services SOW and Appendix C (*Mainframe Hardware List*) of such SOW in consultation with the Province;

(e) confirm, in consultation with the Province, the plan for concurrent migration of Servers (Applications and associated data) (the "**Mainframe Migration Waves**") that should be co-located with the Mainframe System to maintain the performance of the Applications operating on the Mainframe System and co-located Servers as identified in Section 15 (*Virtualization and Migration Project*) of this Transformation SOW;

(f) provide the system integration requirements with the Current MF Provider including for data replication (DASD mirroring) and for the hardware and network connections to the Current MF Provider DASD to support the data migration from the Current MF Provider data centre S. 15
At issue for Inquiry

(g) prepare, in consultation with the Province, an outline of the test plans for Mainframe Services Migration that will include the Mock 0 Test, the Mock 1 Test and the actual migration;

(h) identify the available dates and select a date in consultation with the Province for the initial test exercise of the Disaster Recovery Plan;

(i) prepare, in consultation with the Province, a plan for the shipment of the Non-DR Tapes to the and their subsequent transformation to encrypted media; At issue for Inquiry

(j) prepare a draft Bridge Plan, in consultation with the Province, based on the activities described above and information acquired by the Service Provider, and provide a copy of the draft Bridge Plan to the Province its review and comments; and

(k) provide written notification to the Province when the Mainframe Operational Assessment and Plan Milestone (see table above) has been achieved.

8.1.3 Province Responsibilities

The Province will:

(a) provide the reports, documentation and custom software code that will be provided by Current MF Provider; and provide specifications for the reports, documentation and custom software code that will be developed by the Service Provider;

(b) provide a list of all security resource definitions in place at the Current MF Provider for Mainframe security;

(c) provide documentation of current operational processes and how they are accessed by Clients and make personnel of the Province and Clients available to assist the Service Provider with the development of the outline for Mainframe Services Migration plan;

(d) update the Mainframe System Software described in the Managed Mainframe Services SOW in consultation with the Service Provider;

(e) develop a plan, in consultation with the Service Provider, for system integration between the Current MF Provider and the Service Provider including for data replication (DASD mirroring) and for the hardware and network connections to the Current MF Provider DASD to support the data migration from the Current MF Provider data centre ; S. 15

At issue for Inquiry

(f) facilitate the participation of the Clients currently obtaining Mainframe services from the Province to: (i) identify the testing and acceptance test criteria that such Clients will require to confirm that the Mainframe Services Migration has been successfully completed; and (ii) confirm their commitments to participate in the migration testing in accordance with the agreed to schedule;

(g) identify to the Service Provider the scope and status of any work-in-progress projects involving the Managed Mainframe Services in sufficient detail for the Service Provider and the Province to consider their impact on the Mainframe Services Migration;

(h) develop a plan, in consultation with the Current MF Provider and the Service Provider, for the phase-out of the Current MF Provider that is integrated with the plans for the Mainframe Services Migration including for the destruction by the Service Provider of the DR Tapes at the Current MF Provider when they are no longer required; and

(i) develop a plan, in consultation with the Service Provider for destruction of the Province's Non-DR Tapes at the after the Service Provider has completed their transformation to encrypted media. At issue for Inquiry

8.1.4 Completion

For the purposes of this SOW, the Mainframe Operational Assessment and Plan Significant Milestones (see table above) will be deemed to be "complete" when the milestone has been achieved.

8.2 Detailed Migration Plan

In this phase of the Mainframe Services Migration Transformation Project, the Service Provider will develop and deliver to the Province a detailed migration plan for the Mainframe Services Migration to the (the "**Mainframe Services Migration Plan**") that includes the following: At issue for Inquiry

(a) describe the activities necessary for the migration of the Managed Mainframe Services at a level of detail necessary to execute the migration, including the fallback contingency (if required), tape shipment, tape data encryption and Disaster recovery;

(b) assign responsibility for each task to the Service Provider, the Province (including Clients) and/or the Current MF Provider;

(c) describe the operating documentation for the Managed Mainframe Services that is to be developed by the Service Provider;

(d) describe the activities to acquire, install and configure the required hardware and software at the and the Disaster Recovery Site. This will include the plan to acquire all software keys required from the software vendors of the Province and the Service Provider in accordance with the Agreement; At issue for Inquiry

(e) describe staff preparation activities including the activities required to prepare the Service Provider Personnel for delivery of the Managed Mainframe Services processes as identified in the Managed Mainframe Services SOW, the activities required to prepare the Managed Mainframe Services section of the Manual in accordance with the requirements for the Manual in the Agreement and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*) and any required training of Province Staff;

(f) describe the activities required to update the Disaster Recovery Plan to document the Service Provider's response to a Disaster that prevents the Service Provider from continuing to deliver the Managed Mainframe Services from the At issue for Inquiry

(g) include the integration of the Mainframe Services Migration Plan and the Mainframe Migration Wave to deal with concurrent migration of Servers (Applications and associated data) that should be co-located with the Mainframe to maintain the performance of the Applications operating on the Mainframe and co-located Servers, in accordance with the applicable Committed Annual Plan;

(h) describe the responsibilities of the Province and the Service Provider in respect of any Work-in-Progress Projects that will be underway at the time of the Mainframe Services Migration and the impact of the projects on the Mainframe Services Migration Plan;

(i) describe the activities required to continue services (the "**Fallback Plan**") in the event the Mainframe Services Migration is not successful;

(j) describe the activities required to convert the BC Mail Plus channel attached printers located at the Province Data Centre to Internet Protocol attached printers connected to the Mainframe System at the

At issue for Inquiry

(k) describe the specific activities required to be performed to migrate the mainframe services, Applications and data, at the time of the transfer, from the Current MF Provider S. 15 At issue for Inquiry

(l) identify a freeze period for changes to Mainframe System hardware and software, during the testing and migration phases of the Mainframe Services Migration;

(m) identify a freeze period during the testing and migration phases of the Mainframe Services Migration, for changes to Applications operating on the Mainframe System;

(n) describe the migration test plans for the Mainframe Services Migration that will include the following:

(i) detailed documentation of all required test cases and the acceptance test criteria;

(ii) detailed test plans for the Mock 0 Test and the Mock 1 Test; and

(iii) detailed test plans for the Fallback Plan; and

(o) describe the processes that will be used to report on and respond to performance or Clients' experience issues identified by the Service Provider or the Province following completion of the Mainframe Services Migration;

(p) describe the activities required to ship the Non-DR Tapes to the
At issue for Inquiry including the identification of the tapes to be shipped, the method and date of their shipment, and contingency plan to recreate the tapes in the event of their unexpected loss or destruction during the shipping process; and

(q) describe the plan for the encryption of data on Non-DR Tapes as they are copied to the Service Provider's media after they are moved to the and their subsequent destruction by the Service Provider. At issue for Inquiry

8.2.2 Additional Service Provider Responsibilities

The Service Provider will, in consultation with the Province:

(a) prepare a plan to develop operating documentation to support the Service Provider's delivery of the Managed Mainframe Services;

(b) prepare a plan detailing procurement, installation, and configuration of the required hardware and software at the and the Disaster Recovery Site; At issue for Inquiry

(c) prepare a training plan for delivery of the Managed Mainframe Services as identified in the Managed Mainframe Services SOW including training of Service Provider Personnel and Province Staff, as required;

(d) provide to the Province a list of the Service Provider Personnel requiring access to the current mainframe system at the Current MF Provider for the purposes of the Mainframe Service Migration;

(e) describe activities required for security in respect of the Managed Mainframe Services including:

(i) identification of Service Provider Personnel requiring access to the Mainframe System environment for the provision of Managed Mainframe Services;

(ii) back-up of the data of support personnel of the Current MF Provider; and

(iii) the suspension and deletion of the support personnel of the Current MF Provider;

(f) prepare a Disaster Recovery Plan to document the Service Provider's response to a Disaster that prevents the Service Provider from continuing to deliver the Managed Mainframe Services from the The Disaster Recovery Plan will be developed following the Service Provider's Disaster Recovery Planning SOW published as Appendix D to the Business Continuity and Disaster Recovery SOW (except that there shall be no time and material charges applicable); At issue for Inquiry

(g) integrate the Mainframe Services Migration Plan and the Mainframe Migration Wave to deal with the concurrent migration of Servers (Applications and associated data) that should be co-located with the Mainframe System to maintain the performance of the Applications operating on the Mainframe System and co-located Servers with focus on integrated testing and coordination of all concurrent migration requirements;

(h) include the consideration of Work-in-Progress Projects, if any were identified, to determine their impact on the Mainframe Services Migration and make any

necessary changes to the Mainframe Services Migration Plan or to request that the Province make any necessary changes to the Work-in-Progress Project plans;

(i) develop a plan to assume responsibility for the Service Provider's portion of any Work-in-Progress Projects immediately following the completion of the Managed Services Mainframe Migration;

(j) develop the Fallback Plan;

(k) describe the activities required to convert the BC Mail Plus channel attached printers located at the Province Data Centre to Internet Protocol attached printers connected to the Mainframe System at the At issue for Inquiry

(l) describe the specific activities required to be performed to migrate the Managed Mainframe Services, Applications and associated data, at the time of transfer, from the Current MF Provider S. 15 At issue for Inquiry

(m) determine the freeze periods that apply to changes of Mainframe System hardware and software and the freeze periods that apply to changes of Clients' Applications;

(n) develop the migration test plans for migration of the mainframe services that will include the following;

(i) detailed documentation of all of the required test cases and the acceptance test criteria;

(ii) detailed test plan for the Mock 0 Test;

(iii) detailed test plan for the Mock 1 Test, including the required participation of Clients for migration testing; and

(iv) detailed test plan for the Fallback Plan;

(o) develop the processes that will be used to report on and respond to performance or Client experience issues identified by the Service Provider or the Province following completion of the Mainframe Services Migration;

(p) develop the activities required to ship Non-DR Tapes to the At issue for Inquiry including the identification of the tapes to be shipped, the date of their shipment, and the plans to identify any tapes that require contingency plans if they are lost or destroyed during the shipping process;

(q) develop the plan for the encryption of data on the Non-DR Tapes as they are copied to the Service Provider's media after they are moved to the At issue for Inquiry

(r) prepare the Mainframe Services Migration Plan, in consultation with the Province, based on the activities described above and information acquired by the Service Provider, and provide a copy of the draft Mainframe Services Migration Plan to the Province for its approval; and

(s) provide written notification to the Province when the Detailed Migration Plan Milestone (see table above) has been achieved

8.2.3 Province Responsibilities

The Province will:

(a) assign a Mainframe Service Migration leader who will be responsible for the Province's participation in the Mainframe Services Migration and have authority to direct the Current MF Provider;

(b) identify the Province Staff who require notification or training about any aspect of changes to the Managed Mainframe Services that affect how the Province accesses or uses the services, if any such changes are required;

(c) communicate the freeze period for hardware, software, and Applications to the Current MF Provider and Clients;

(d) obtain access for the Service Provider Personnel requiring access to the current mainframe system at the Current MF Provider, as identified by the Service Provider;

(e) designate the Province Staff to be identified as performing the Province roles identified in the Disaster Recovery Planning SOW published as Appendix D to the Business Continuity and Disaster Recovery SOW;

(f) identify: (i) the Province Staff accountable for Work-in-Progress Projects, if any were identified; (ii) who will be assigned to provide the Service Provider with information about the projects, including scope, commitments, plans and status; and (iii) who will also be authorized to agree to changes to the Province Work-in-Progress Project plans where appropriate to do so. To the extent that it is agreed through the Change Order Process described in the Agreement that the Service Provider will accept responsibility for a Work-in-Progress Project or part thereof, the Province will also designate Province Staff to assist the Service Provider with developing its plan to assume such responsibility;

(g) designate the Province Staff who will be assigned to Province roles in the Fallback Plan with respect to the testing and possible execution of the Fallback Plan in the event the Mainframe Services Migration is not successful;

(h) designate the Province Staff who: (i) will be assigned the Province roles in the actual transfer of the Mainframe Servers, Applications and data; and (ii) who have

authority and accountability to engage Clients as necessary to complete the Mainframe Services Migration;

(i) designate the Province Staff: (i) who will be assigned to the Province roles in the Mainframe Services Migration testing; and (ii) who have authority and accountability to engage Clients, as necessary, to support development of the test cases and their acceptance criteria and to participate in executing the Mock 1 Test;

(j) designate the Province Staff who will assist the Service Provider with designing the processes that will be used to report on and respond to performance or Client experience issues;

(k) provide to the Service Provider a list of authorized Province Staff who are authorized to modify batch schedule(s);

(l) provide to the Service Provider a list of approved Persons as they relate to Client Removable Media Support Services (as defined in the Managed Mainframe Services SOW);

(m) approve access to the Mainframe System environment for Service Provider Personnel requiring access for the Service Provider's provision of the Managed Mainframe Services;

(n) delete the access of the support personnel of the Current MF Provider to the Mainframe System;

(o) designate the Province Staff who will assist the Service Provider with development of the shipping plan and any contingency plans for the Non-DR Tapes and who have authority and accountability to engage and direct the Current MF Provider in support of these activities; and

(p) designate the Province Staff who will assist the Service Provider with development of the plan to convert the BC Mail Plus channel attached printers located at the Province Data Centre to Internet Protocol attached printers connected to the Mainframe System at the

At issue for Inquiry

8.2.4 Completion

For the purposes of this SOW, the Detailed Migration Plan Significant Milestones (see table above) will be deemed to be "complete" when the milestone has been achieved.

8.3 Execution of the Detailed Migration Plan

8.3.1 Plan Execution

The Service Provider and the Province will execute the Mainframe Services Migration Plan in accordance with the provisions of this Section 8. In addition, the Mainframe Services Migration Plan will be tracked and reported by the Service Provider as described in Section 16 (*Transformation Management and Governance*) of this SOW and reported through the Governance Process.

In the event that any task, phase, or deliverable from the Mainframe Services Migration Plan is not completed by the date specified in the Mainframe Services Migration Plan, the Parties will continue to work towards expediting the migration, as contemplated in this Section 8. In addition, either Party can make a claim against the other Party for their costs incurred due to a delay, if the delay is more than two months past the scheduled migration, as determined from the Mainframe Services Migration Plan developed. If the delay is less than two months, each Party shall cover their own costs resulting from such a delay.

8.3.2 Progress Reviews

8.3.2.1 Mainframe Operation Assessment and Plan – Progress Reviews

The Parties will meet to review the progress of the Mainframe Services Migration project as follows:

(a) the Parties will meet monthly commencing six months prior to the Bridge Plan deliverable date to review the status of the Mainframe Services Migration project and the Service Provider's progress as against the Transformation Plan; and

(b) the Parties will meet twice each month, commencing three months prior to the Bridge Plan deliverable date to review the Service Provider's progress as against the Transformation Plan.

If at any time the actual progress of the Service Provider has significantly fallen behind schedule or the Province is of the opinion that the actual progress of the Service Provider has significantly fallen behind schedule or that the Bridge Plan will not be completed by the deliverable date for the Bridge Plan , then the Service Provider will be required:

(c) within ten Business Days of receipt of notice from the Province, to produce and deliver to the Province:

  (i) a report identifying the reasons for the delay; and

  (ii) a plan showing the steps that are to be taken by the Service Provider to complete the Bridge Plan by the deliverable date for the Bridge Plan (the "**Bridge Remedial Plan**"); and

(d) to work diligently to bring completion of the Bridge Plan by the deliverable date for the Bridge Plan back on schedule in accordance with the Bridge Remedial Plan approved by the Province.

The Service Provider will notify the Province if, at any time, the actual progress of the Mainframe Services Migration project is significantly ahead of schedule.

8.3.2.2 Mainframe Migration Progress Reviews

Commencing twelve months prior to the Managed Mainframe Services Commencement Date and continuing until the completion of the Mainframe Services Migration project the Parties will meet monthly. If the Service Provider is behind schedule for the Mainframe Services Migration project, then:

(a) the Parties will meet weekly to review the status of the Service Provider's progress to complete and execute the Mainframe Services Migration Plan;

(b) the Service Provider will review its progress prior to each weekly meeting and will report to the Province on the measures that are being implemented in response to the delays; and

(c) the Province and the Service Provider will cooperate to identify any actions that may be taken by any of them in response to the delays and, as they deem appropriate, in investigating alternate solutions.

If the delay in the Mainframe Services Migration project is, at any time determined to be, one month or more, then the Parties will immediately escalate the issue of the delays to the Joint Executive Committee under the Agreement. The Province and the Service Provider will continue to review the delay at Joint Executive Committee meetings on a bi-weekly basis until such time as the delays have been eliminated and the Mainframe Services Migration project is back on schedule.

8.3.3 Countdown Review

The Parties acknowledge and agree that the following periods are critical check points (the "**Critical Check Points**") for the Mainframe Services Migration project:

- ten months;
- seven months; and
- three months

prior to the Managed Mainframe Services Commencement Date. If the Mainframe Services Migration project is determined to be delayed or the Province is of the opinion that the Mainframe Services Migration project is delayed then the Service Provider shall prepare a Migration Remedial Plan as described in Section 8.3.4.3 below for review by the Parties at the Joint Executive Committee.

8.3.4 Migration Remedial Plan

If at the Critical Checkpoints the Mainframe Services Migration project is delayed, then the Service Provider shall:

(a) immediately provide the Province with a reasonable plan and schedule (the "**Migration Remedial Plan**") to mitigate the effect of such delay, which schedule shall specify in reasonable detail the manner in, and the latest date by which, such delay is proposed to be mitigated and the Mainframe Migration Plan will be available; and

(b) thereafter, perform its obligations to achieve all elements of the Migration Remedial Plan in accordance with its terms within the time for the performance of its obligations thereunder.

The Service Provider will deliver to the Province a Migration Remedial Plan that identifies options available to respond to the delays. The Province shall not be required to accept any option proposed by the Service Provider and shall accept one of the options proposed by the Service Provider only if it is acceptable to the Province.

If the Service Provider fails to put forward the Migration Remedial Plan, or the delay is not remedied within the requisite period, or the Service Provider puts forward a Migration Remedial Plan and fails to perform its obligations thereunder necessary to achieve all elements of the Migration Remedial Plan in accordance with its terms within the requisite time, or the Province does not accept any of the options proposed by the Service Provider in the Migration Remedial Plan, then in each such case the matter will be escalated to the Joint Executive Committee in accordance with its Governance Process.

8.3.5 Fall Back Contingency

In the event the Mainframe Services Migration is not successful and the Parties elect to postpone the Mainframe Services Migration, the Service Provider and the Province will execute the Fallback Plan.

8.3.6 Completion

For the purposes of this SOW, the Execution of the Detailed Migration Plan Significant Milestones (see table above) will be deemed to be "complete" when all the milestones within the Detailed Migration Plan have been achieved as per the Detailed Migration Plan prepared and approved by the Parties.

8.4 Potential Future Transformation Projects

The Parties have identified optional Managed Mainframe Services transformation projects to be considered for possible implementation, following the Mainframe Service Migration, including the following projects (to be implemented in accordance with the Change Order Process):

(a) Mainframe Software Rationalization;

(b) Mainframe Reporting Review and Rationalization;

(c) Mainframe Storage Management Review;

(d) Replacement of Custom S. 15

(e) Enablement of Secure S15 and

(f) Consideration of New Mainframe Technologies.

The potential scope of such projects is described below. The scope of such projects will be confirmed, following the Mainframe Services Migration but prior to implementation.

The Service Provider and the Province will cooperate during the design phase of these potential projects to agree on the design in consultation with the Technology Architecture Working Group for review of design compliance with the Province's enterprise architecture and standards.

8.4.2 Mainframe Software Rationalization

If the Province elects to proceed with the Mainframe Software Rationalization project, the Service Provider will:

(a) review the usage of the Software products licensed by the Province; and

(b) make recommendations that will result in lower costs for the Province and Clients, including the retirement of such products or the replacement thereof with alternative Software products performing similar functions at a reduced cost.

The Province will review the Service Provider's recommendations.

8.4.3 Mainframe Reporting Review and Rationalization

If the Province elects to proceed with the Mainframe Reporting Review and Rationalization project, the Service Provider will:

(a) review the usage of the reports requested and/or being provided to the Province;

(b) review the information contained in the reports for relevance; and

(c) make recommendations to improve the relevance or utility of such reports for the Province and Clients or to eliminate certain reports, with a view to rationalizing or reducing the number of such reports.

The Province will review the Service Provider's recommendations.

8.4.4 Mainframe Storage Management Review

If the Province elects to proceed with the Mainframe Storage Management Review project, the Service Provider will:

(a) review the Province's current storage management procedures and policies;

(b) review the storage management compliance, costs and ease of use for Clients; and

(c) make recommendations for improvements.

The Province will review the Service Provider's recommendations.

8.4.5 Replace Custom Network Solicitor (NETSOL)

If the Province elects to proceed with the Replace Custom Network Solicitor (NETSOL) project, the Service Provider will:

(a) review the Province's current custom developed application for Mainframe System access; and

(b) make recommendations on potential commercial off the shelf (COTS) products to replace such application.

The Province will review the Service Provider's recommendations.

8.4.6 Enablement of Secure S15

If the Province elects to proceed with the Enablement of Secure S15 project, the Service Provider will assess the Mainframe System environment and make a recommendation to the Province on the enablement of secur S15 access for Clients.

The Province will review the Service Provider's recommendations.

8.4.7 Consideration of New Mainframe Technologies

The Parties may agree to implement, by way of a project under the Change Order Process, any recommendations made by the Service Provider concerning new mainframe technologies as defined in the Mainframe Client Technical Support Services Section of the Managed Mainframe Services SOW, including for example any such recommendations made by the Service Provider with respect to:

(a) applicability of ZiiP and/or ZaaP specialty engines;

(b) use of zLinux;

(c) new developer tools; or

(d) Service Oriented Architecture (SOA) developments.

9. SERVER SYSTEMS MANAGEMENT TRANSFORMATION

Server Systems Management is the operation support, monitoring and administration of the non-Mainframe Servers operating Windows, AIX, Solaris, Linux or OpenVMS Operating Systems.

Pursuant to the Server Systems Management Transformation Project, the Service Provider will transform the Server Systems Management of the Province Servers by:

(a) creating new Server system administration manuals for the Province Servers;

(b) adding its Server Systems Management tools to the Province Servers;

(c) conducting an initial virus scan of the Province Servers; and

(d) conducting an initial security policy compliance scan of the Province Servers.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Server Systems Management Transformation	Service Provider Toolkit Implemented on Servers at Province Data Centres	Software and Patch Distribution Tools	See Schedule 23 (*Fees*), Appendix I	Month 1-4, April, 2009 - July, 2009	**Service Provider Toolkit installed on all eligible servers** **Service Provider software distribution and patch management processes are implemented** **Service Provider monitoring processes implemented** **Systems Administration operating documentation current for all Province servers**
		Server Monitoring Tools	See Schedule 23 (*Fees*), Appendix I	Month 1-6, April, 2009 – September, 2009	
		Backup Management and Storage Management Tools	See Schedule 23 (*Fees*), Appendix I	Month 2, May, 2009	
		Server Administration Servers	See Schedule 23 (*Fees*), Appendix I	Month 2, May, 2009 (to be confirmed)	
		Anti-Virus Tools	See Schedule 23 (*Fees*), Appendix I	Month 3, June, 2009	
		Security Policy Compliance Management Tools	See Schedule 23 (*Fees*), Appendix I	Month 3, June, 2009	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
	Prepare Staff	Server Systems Management Operating Manual and Server System Administration Manuals	See Schedule 23 (*Fees*), Appendix I	Month 1-6, April, 2009 – September, 2009	**Server Management section of the Manual completed** **Support staff trained**
		SQL Server 2008 Training	See Schedule 23 (*Fees*), Appendix I	Month 7, October, 2009	
	Virus Scan	Initial Anti-Virus Scan for Province Servers	See Schedule 23 (*Fees*), Appendix I	Month 4, July, 2009	**Service Provider reports to Province on results and remediates any viruses found**
	Security Compliance Scan	Initial Security Policy Compliance Scan on Servers	See Schedule 23 (*Fees*), Appendix I	Month 6, September, 2009	**Service Provider reports to Province on security compliance findings**
	Service Provider Toolkit extended to STMS Calgary Data Centre	Software and Patch Distribution Tools	See Schedule 23 (*Fees*), Appendix I	Month 8, November, 2009	**Service Provider Toolkit resources ready to support migration of Servers (Applications and data) to STMS Calgary Data Centre**
		Anti-Virus Tools	See Schedule 23 (*Fees*), Appendix I	Month 9, December, 2009	
		Event Log Collection Tools	See Schedule 23 (*Fees*), Appendix I	Month 9, December, 2009	
		Network Tools	See Schedule 23 (*Fees*), Appendix I	Month 9, December, 2009	
		Backup Management and Storage Management Tools	See Schedule 23 (*Fees*), Appendix I	Month 9, December, 2009	
		Server Monitoring Tools	See Schedule 23 (*Fees*), Appendix I	Month 9, December, 2009	
	Service Provider Toolkit extended to STMS Interior Data Centre	Software and Patch Distribution Tools	See Schedule 23 (*Fees*), Appendix I	Month 25, April, 2011	**Service Provider Toolkit resources ready to support migration of Servers (Applications and data) to STMS Interior Data Centre**
		Anti-Virus Tools	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	
		Event Log Collection Tools	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
		Network Tools	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	
		Backup Management and Storage Management Tools	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	
		Server Monitoring Tools	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	
	Shared File and Print Project	Shared File and Print Project	N/A	To be determined during initial refinement of the Transformation Plan	**Concurrence on project plan, requirements, design, tests, and test acceptance criteria.**

9.2 Install Standard Tools at Province Data Centres

In this phase of the Server Systems Management Transformation Project, the Service Provider will install its Server Systems Management tools on Province Servers.

Further to the operation of the Service Provider's standard Server Systems Management tools described in Section 9.2 (*Install Standard Tools at Province Data Centres*), the Province will make changes, as may be necessary, to its network environment including firewall rule changes, in order to allow the tools to be installed and to function. The changes are described in the Server Install section of the Server Management Services SOW and will be processed through the Change Management Process as required for the testing, deployment, and ongoing operation of these tools.

9.2.1 Software and Patch Distribution Tools

To implement the Service Provider's Software and Patch Distribution Tools, the Service Provider will:

(a) install the Service Provider's tool Servers for the Software and Patch Distribution Tools in Province Data Centres;

(b) test the installation of Software Agents on Province Servers; and

(c) deploy Software Agents on Province Servers.

9.2.1.2 Installation of Tool Servers

In accordance with the procedures set out in the Server Management Services SOW, the Service Provider will:

(a) install its tool Servers for the Software and Patch Distribution Tools at such Province Data Centre as is agreed to by the Province and the Service Provider promptly following the Hand-Over Date; and

(b) connect the tool Servers via the Management Network to support the provisioning of Software updates and patches.

The Province will cooperate with the Service Provider to enable the Service Provider to install its tool Servers at the agreed to Province Data Centre and to connect its tool Servers via the Management Network.

9.2.1.3 Testing

9.1.1.2.1 Service Provider Responsibilities

Prior to the installation of any Software Agents for the Software and Patch Distribution Tools on the Province Servers, the Service Provider will test deployment of the Software Agents in the Province lab at the Province Data Centre S. 15 The Service Provider will also conduct tests in the Province lab to test the removal, from the Province Servers, of any Province software and patch distribution technology currently operating on the Province Servers. The objective of these tests is to demonstrate that the Service Provider's Software and Patch Distribution Tools can be installed and operated safely on the Province Servers using the automated agent deployment technology that is part of the Software and Patch Distribution Tool.

Following successful completion of the deployment tests in the Province lab, the Service Provider will conduct a "pilot" on a limited number of the Province Servers. Pilot testing will follow the Change Management Process described in the Service Management SOW. The objective of the Pilot test is to demonstrate the safe operation of the automated agent deployment technology that is part of the Software and Patch Distribution Tools in the Province's current Server environment.

The Service Provider will:

(a) work with the Province to define test cases and acceptance test criteria for a deployment test in the Province lab and for the pilot; and

(b) conduct the deployment test and pilot with the Province so as to meet the agreed to test criteria.

9.1.2.2.2 Province Responsibilities

The Province will:

(c) provide access to the Province lab located S. 15 as required for the deployment test in the Province lab and for the pilot;

(d) work with the Service Provider to define test cases and acceptance test criteria for a deployment test in the Province lab and for the pilot; and

(e) accept the results of the deployment test and pilot when the results meet the agreed to acceptance criteria.

9.2.1.4 Installation

Following the Province's acceptance of the results of the deployment and pilot tests, the Service Provider in consultation with the Province will schedule deployment of the Software Agents for the Software and Patch Distribution Tools for the Province Servers. Software and Patch Distribution agent deployment will follow the Change Management Process described in the Service Management SOW.

The Service Provider will:

(a) inform the Province's Network operations team of network changes needed for the Software Agents to communicate with the Service Provider's Software and Patch Distribution Tools Servers; and

(b) provide written notification to the Province when the Software and Patch Distribution Tools Milestone (see table above) has been achieved including when:

(i) the deployment of the Software Agents is completed;

(ii) the Service Provider's Software Distribution and Patch Tools are operational; and

(iii) the Province's software distribution and patch technology has been retired.

The Province will make the changes to its network environment, including firewalls, as necessary in order for the Software Agents to communicate with the Software and Patch Distribution Tools Servers.

The Service Provider and the Province acknowledge that there will be Province Servers that are incompatible with the Service Provider's Software Distribution and Patch Tools technology and that the Parties will cooperate to develop work arounds so that such incompatibilities do not prevent deployment of the Software Agents generally.

9.2.2 Server Monitoring Tools

To implement the Service Provider's Server Monitoring Tools, the Service Provider will:

(a) install tool servers in the Province Data Centres;

(b) test the installation of Software Agents on Province Servers; and

(c) deploy Software Agents on Province Servers.

9.2.2.2 Installation of Tool Servers

In accordance with the procedures set out in the Server Management Services SOW, the Service Provider will:

(a) install its tool Servers for its Server Monitoring Tools at such Province Data Centres as is agreed to by the Province and the Service Provider promptly following the Hand-Over Date; and

(b) connect the tool Servers via the Service Provider's Management Network to support the remote monitoring of Servers from the Service Provider Support Locations.

The Province will cooperate with the Service Provider to enable the Service Provider to install its tool Servers at the agreed to Province Data Centre and to connect its tool Servers via the Service Provider's Management Network.

9.2.2.3 Testing

9.1.2.2.1 Service Provider Responsibilities

Prior to the installation of the Software Agents for the Server Monitoring Tools on the Province Servers, the Service Provider will test the deployment of the Software Agents in the Province lab at the Province Data Centre S. 15 . The Service Provider will also conduct tests in the Province lab to test the removal, from the Province Servers, of any Province server monitoring technology currently operating on the Province Servers. The objective of these tests is to demonstrate that the Service Provider's Server Monitoring Tools can be installed and operated safely on the Province Servers.

Following successful completion of the deployment tests in the Province lab, the Service Provider will conduct a "pilot" on a limited number of the Province Servers. Pilot testing will follow the Change Management Process described in the Service Management SOW. The objective of the pilot test is to demonstrate the safe operation of the Service Provider's Server Monitoring Tools in the Province's current Server environment.

The Service Provider will:

(a) work with the Province to define test cases and acceptance test criteria for a deployment test in the Province lab and for the pilot; and

(b) conduct the deployment test and pilot with the Province so as to meet the agreed to test criteria.

9.1.2.2.2 Province Responsibilities

The Province will:

(c) provide access to the Province lab located at S. 15 lab as required for a deployment test in the Province lab and for the pilot;

(d) work with the Service Provider to define test cases and acceptance test criteria for a deployment test in the Province lab and for the pilot; and

(e) accept the results of the deployment test and pilot when the results meet the agreed to acceptance criteria.

9.2.2.4 Installation

Following the Province's acceptance of the results of the deployment and pilot tests, the Service Provider in consultation with the Province will schedule deployment of the Software Agents for the Server Monitoring Tools for the Province Servers. Server Monitoring Tools agent deployment will follow the Change Management Process described in the Service Management SOW.

The Service Provider will:

(a) inform the Province's Network operations team of network changes needed for the Software Agents to communicate with the Software and Patch Distribution Tools Servers; and

(b) provide written notification to the Province when the Server Monitoring Tools Milestone (see table above) has been achieved, including when:

(i) the deployment of the Software Agents is completed;

(ii) the Service Provider's Server Monitoring Tools are operational; and

(iii) the Province's Server monitoring technology has been retired.

The Province will make the changes to its network environment, including firewalls, as necessary in order for the Software Agents to communicate with the Server Monitoring Tools Servers.

The Service Provider and the Province acknowledge that there will be Province Servers that are incompatible with the Service Provider Server Monitoring Tools technology and that the Parties will cooperate to develop work arounds so that such incompatibilities do not prevent deployment of the Software Agents generally.

9.2.3 Backup Management Tools

The Service Provider will use the Province's existing Software backup management tools for managing backup services on Province Servers.

Any Servers installed by the Service Provider will have backup Software Agents that are compatible with the Province backup management tools at the Province Data Centres.

9.2.4 Storage Management Tools

Software storage management tools refer to the Software tools that are used to manage storage devices.

The Service Provider will use the Province's existing Software storage management tools to manage Province storage devices. If necessary, the Service Provider will re-configure the Province's existing Software storage management tools for compatibility with the Service Provider's updated storage operating processes as described in the Managed Storage and Managed Backup SOW.

The Service Provider will retire Province Software storage management tools that are not required for the Service Provider's updated storage operating processes.

The Service Provider will install its own Software storage management tools for management of Service Provider storage devices.

To implement the Service Provider's Software storage management tools for use at Province Data Centres, the Service Provider will:

(a) install Service Provider storage management tool Servers for the Service Provider Software storage management tools at Province Data Centres; and

(b) install Service Provider Software storage management tools on the Service Provider storage management tools Servers at the Province Data Centres.

9.2.4.2 Installation of Storage Management Tool Servers

In accordance with the procedures set out in the Server Management Services SOW, the Service Provider will install its tool Servers for the Software storage management tools at such Province Data Centre as is agreed to by the Parties promptly following the Hand-Over Date.

The Province will cooperate with the Service Provider to enable the Service Provider to install its tool Servers at the agreed to Province Data Centre.

9.2.4.3 Installation of Storage Management Tools

The Service Provider will install its Software storage management tools on the storage management tool Servers installed by the Service Provider at Province Data Centres.

The Service Provider will provide written notification to the Province when the Backup Management and Storage Management Tools Milestone (see table above) has been achieved (when the storage management tool deployment is complete and fully operational).

9.2.5 Server Administration Servers

The Service Provider utilizes administration Servers (use of Service Provider Citrix software and Servers is currently contemplated) to enable Service Provider system administrators to manage

the Servers for which they are responsible without allowing direct access to the Province's production Servers.

The Service Provider will be responsible for installing the administration Servers within the Service Provider network environment.

The Service Provider will provide written notification to the Province when the Server Administration Servers Milestone (see table above) has been achieved (when the Servers have been installed within the Service Provider network environment).

9.2.6 Anti-Virus Tools

The Service Provider will install its anti-virus management Software on Service Provider tool Servers at such Province Data Centre as is agreed to by the Parties promptly following the Hand-Over Date. This Software manages anti-virus software operating on Service Provider Servers. The anti-virus Software operating on Service Provider Servers supports the scanning, detection, logging and removal of viruses, worms and similar contaminants from Service Provider Servers. New Servers provided by the Service Provider will be free of any known virus infections when they are initially put into service as described in the Server Management Services SOW.

With respect to the Province Servers, the Service Provider will:

(a) utilize the Province's existing anti-virus infrastructure to manage anti-virus activities for Province Servers;

(b) conduct a review of all of the Province Servers to determine if the Server requires anti-virus software; and

(c) for those servers requiring anti-virus Software:

  (i) if the anti-virus software is not currently installed, install the Province's anti-virus software as required by the Server (note: most Unix Servers do not require Anti-Virus software); and

  (ii) if the anti-virus Software is not up-to-date, update the Province anti-virus software and signature files.

The Service Provider will provide written notification to the Province when the Anti-Virus Tools Milestone (see table above) has been achieved (when the anti-virus Software installed on Province Servers is up-to-date, uses up-to-date signature files and is operational).

9.2.7 Security Policy Compliance Management Tools

The Service Provider's security policy compliance management tools ("**PCM Tools**") initiate security policy compliance scans on Servers, collect the results, and produce reports for analysis of compliance to agreed Security Policies as described in the Security SOW.

The Service Provider will install its PCM Tools within the Service Provider's Canadian network environment.

The PCM Tools require that Software Agents be deployed on Province Servers. The Service Provider will test and deploy the Software Agents for the PCM Tools on the Province Servers as part of the testing and deployment of the Software Agents for the Server Monitoring Tools described in Section 9.2.2 (*Server Monitoring Tools*).

The Service Provider will provide written notification to the Province when the Security Policy Compliance Management Tools Milestone (see table above) has been achieved (when the PCM Tool deployment is completed and is fully operational).

9.2.8 Completion

For the purposes of this SOW, the Service Provider Toolkit Implemented on Servers at Province Data Centres Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.2 (*Install Standard Tools at Province Data Centres*) have been achieved.

9.3 Prepare Staff

9.3.1 Update Operating Documentation

The Midrange section of the Manual (referred in the Server Management Services SOW as the Midrange Operating Manual) sets out the specific operating procedures, processes, tasks and functions that are required to be performed by the Service Provider to deliver the Server Systems management services.

At the Hand-Over Date, the Service Provider will utilize the Province's existing manual for the Server Systems management services (described in the Server Management Services SOW).

The Service Provider will develop the Midrange section of the Manual in accordance with the Agreement, and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*), as the Province procedures are revised in connection with the implementation of the Service Provider's operating procedures.

The Service Provider will provide written notification to the Province when the Server Systems Management Operating Manual and Server System Administration Manuals Milestone (see table above) has been achieved (when the Midrange section of the Manual describes the Server Systems management services being provided by the Service Provider from the Province Data Centres).

9.3.2 Training

The Service Provider will train the Service Provider Personnel in the Service Provider's operating procedures as documented in the Midrange section of the Manual as the Provinces procedures are revised in connection with the implementation of the Service Provider's operating procedures.

The Service Provider will train the Service Provider Personnel who support Microsoft SQL Server in preparation for the use by the Province of Microsoft SQL Server 2008.

9.3.3 Completion

For the purposes of this SOW, the Prepare Staff Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.3 (*Prepare Staff*) have been achieved.

9.4 Perform Initial Anti-Virus Scan

When the anti-virus Software is deployed as described in Section 9.2.6 (*Anti-Virus Tools*) above, the Service Provider will utilize the anti-virus tools to schedule and execute scans on all existing Province Servers at a time or times that are acceptable to the Province.

If the scans on the Province Servers detect any virus, worms or similar contaminants on any Province Servers, the Service Provider will notify the Province thereof and take remedial action through the Change Management Process described in the Service Management SOW.

The Service Provider will provide written notification to the Province when the Initial Anti-Virus Scan for Province Servers Milestone (see table above) has been achieved (when the initial anti-virus scan and any resulting virus remediation is completed in respect of all Province Servers).

9.4.1 Completion

For the purposes of this SOW, the Initial Anti-Virus Scan for Province Servers Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.4 (*Perform Anti-Virus Scan*) have been achieved.

9.5 Perform Initial Security Policy Compliance Scan

When the Service Provider's PCM Tools are deployed as described in Section 9.2.7 (*Security Policy Compliance Management Tools*), above, the Service Provider will utilize the PCM Tools to scan all existing Province Servers and assess the results to determine if they are in compliance with the agreed Security Policy as described in the Security SOW.

The Service Provider will provide the Province with policy compliance reports.

The Service Provider will provide written notification to the Province when the Initial Security Policy Compliance Scan on Servers Milestone (see table above) has been achieved (when the initial policy compliance scan activity is completed).

The Service Provider will scan all new servers for security policy compliance at the time of installation as described in the Server Management Services SOW.

9.5.1 Completion

For the purposes of this SOW, the Security Compliance Scan Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.5 (*Perform Initial Security Policy Compliance Scan*) have been achieved.

9.6 Install Standard Tools at STMS Data Centres

The Service Provider will install and host at the STMS Data Centres instances of its standard tool Servers, which include as follows:

(a) Software and patch distribution tools Servers;

(b) Server monitoring tools Servers;

(c) storage and backup tools Servers; and

(d) anti-virus tools on the software and patch distribution tools Servers.

These are additional instances of the Service Provider's tool Servers that were previously described in Section 9.2 (*Install Standard Tools at Province Data Centres*).

The Service Provider will provide written notification to the Province when the Software and Patch Distribution Tools Milestone (see table above), the Server Monitoring Tools Milestone (see table above), the Backup Management and Storage Management Tools Milestone (see table above), and the Anti-Virus Tools Milestone (see table above) have been achieved (when each of such tools have been installed at the STMS Data Centres).

The Service Provider will also install network tool Servers that support monitoring and management of network devices, and allow for the creation and management of VLANs and firewall rules. Such network tool Servers will be connected to the Service Provider's management network to support remote monitoring and management of the Service Provider's network equipment from other Service Locations in Canada. Such network tool Server will also be able to communicate with all tools Servers on Service Provider's network and the Province's network. The Province will work cooperatively with the Service Provider to complete necessary Province router and firewall rule changes to support the communication with all Service Provider tools Servers on Service Provider's network and the Province's network.

The Service Provider will provide written notification to the Province when the Network Tools Milestone (see table above) has been achieved (when the network tool Servers have been installed and connected to the Service Provider's management network).

The Service Provider will also install event log collection servers (more commonly known as "SYSLOG" Servers as described in the Security SOW) that support the event log collection from Servers and network devices and store them in a central repository.

The Service Provider will provide written notification to the Province when the Event Log Collection Tools Milestone (see table above) has been achieved (when the event log collection servers have been installed).

9.6.2 Completion for STMS Calgary Data Centre

The Service Provider will provide written notification to the Province when tools referred to in Section 9.6 (*Install Standard Tools at STMS Data Centres*) are fully operational at the STMS Calgary Data Centre).

For the purposes of this SOW, the Service Provider Toolkit extended to STMS Calgary Data Centre Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.6 (*Install Standard Tools at STMS Data Centres*) have been achieved.

9.6.3 Completion for the STMS Interior Data Centre

The Service Provider will provide written notification to the Province when the tools referred to in Section 9.6 (*Install Standard Tools at STMS Data Centres*) are fully operational at the STMS Interior Data Centre.

For the purposes of this SOW, the Service Provider Toolkit extended to STMS Interior Data Centre Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.6 (*Install Standard Tools at STMS Data Centres*) have been achieved.

9.7 Shared File and Print Project

This phase of the Server Systems Management Transformation Project will reduce the cost to deliver the Shared File Print (SFP) service, as described in the Shared File and Print Services SOW.

The Province and the Service Provider agree as follows:

(a) the objectives of the Shared File and Print Project are to improve the reliability of the Province Shared File and Print infrastructure while permitting the Service Provider to reduce the costs of providing the Shared File and Print service in keeping with pricing assumptions; and

(b) the transformed Shared File and Print service must provide end client experience and functions that are equal to or better than the existing Shared File and Print service.

9.7.2 Joint Responsibilities

The Province and the Service Provider, working jointly, will:

(a) identify Province Business Requirements;

(b) develop functional requirements, such as:

(i) maintaining existing performance; and

(ii) Server recovery time objectives; and

(c) agree on the design.

9.7.3 Service Provider Responsibilities

The Service Provider will:

(a) develop a detailed project plan in consultation with the Province including requirements for Province participation;

(b) develop such requirements and in consultation with the Province;

(c) develop the design in cooperation with the Province and consult with the Technology Architecture Working Group for review of design compliance with the Province's enterprise architecture and standards;

(d) procure, prepare, and install hardware, software, or third party services as required by the detailed project plan and the design;

(e) work with the Province to define the test cases and acceptance test criteria for the Shared File and Print project;

(f) prepare required updates for the Midrange section of the Manual in accordance with the requirements for the Manual in the Agreement and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*);

(g) conduct the agreed testing in cooperation with the Province;

(h) upon completion of the implementation and testing activities including achievement of all acceptance test criteria, provide notice to the Province that the Shared File and Print Project Milestone (see table above) has been achieved when it is ready to commence deployment of the transformed Shared File and Print services; and

(i) upon approval of the Province for commencement of the deployment of the transformed Shared File and Print services, commence implementation of the transformed Shared File and Print services as described by the implementation plan.

9.7.4 Province Responsibilities

The Province will:

(a) facilitate the required participation of the Province and Clients as agreed with the Service Provider in the detailed implementation plan;

(b) develop the design in cooperation with the Service Provider and consult with the Technology Architecture Working Group for review of design compliance with the Province's enterprise architecture and standards;

(c) work with the Service Provider to define test cases and acceptance test criteria for the Shared File and Print project; and

(d) conduct the agreed to testing in cooperation with the Service Provider.

9.7.5 Completion

For the purposes of this SOW, the Shared File and Print Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 9.7 (*Shared File and Print Project*) have been achieved.

10. VIRTUALIZATION ASSESSMENT AND MIGRATION PLANNING PROJECT

The purpose of the Virtualization Assessment and Migration Planning Project is to develop an agreed to multi-year plan (the "**Multi-Year Plan**") for the migration of Province Applications from the existing Province Servers to Virtual or Physical Servers provided by the Service Provider.

For the purpose of this Transformation Program, "**Virtualization**" means installing multiple images of Servers on one Physical Server with each image maintaining the appearance and capabilities of the Operating System from which it was derived without being constrained by or dependant upon the Physical Server on which it operates. Applications that formerly were hosted on Physical Servers are said to run on a "**Virtual Server**" after they are "**Virtualized**".

The Virtualization Assessment and Migration Planning Project will be performed by the Service Provider in the following phases:

(a) Project Planning;

(b) Virtualization and Migration Test Lab;

(c) Virtualization Assessment and Migration Study;

(d) Multi-Year Plan; and

(e) First Committed Annual Plan.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Virtualization Assessment and Migration Planning Project	**Virtualization Assessment and Migration Planning for all Servers**	Virtualization Assessment and Migration Planning Project Plan	See Schedule 23 (*Fees*), Appendix I	Month 1, April, 2009	**Virtualization Assessment and Migration Planning completed for all Province Applications and their associated data** **Multi-Year Plan accepted and agreed to** **Province and Service Provider commitment to content of first Committed Annual Plan** **Identification of Applications and their associated data that must migrate concurrent with Mainframe Services Migration**
		Virtualization Assessment and Migration Test Lab	See Schedule 23 (*Fees*), Appendix I	Month 2, May, 2009	
		Virtualization Assessment and Migration Study	See Schedule 23 (*Fees*), Appendix I	Month 1-3, April-June, 2009	
		Virtualization Assessment and Migration Planning Project Plan Approved	See Schedule 23 (*Fees*), Appendix I	Month 5, August, 2009	
		First Committed Annual Plan for August 2009-March 2010 (first 2 Virtualization and Migration Waves)	N/A	Month 5, August, 2009	

10.2 Project Planning

10.2.1 Service Provider Responsibilities

In this phase of the Virtualization Assessment and Migration Planning Project, the Service Provider will:

(a) develop a project plan for the Virtualization Assessment and Migration Planning Project (the "**Virtualization Assessment and Migration Planning Project Plan**") that will describe the phases, activities, tasks, Province participation requirements, milestones and deliverables required to complete the Virtualization

Assessment and Migration Planning Project, and identify risks associated with the Virtualization and Migration and methods to mitigate such risks;

(b) clarify the scope of work for the Virtualization Assessment and Migration including the impact of the following:

(i) constraints of the Clients;

(ii) geographic locations;

(iii) activities and schedule; and

(iv) Province and Service Provider resources and availability;

(c) identify and obtain, with the assistance of the Province, the information required to clarify the scope of work;

(d) develop the Virtualization Assessment and Migration Planning Project Plan including the requirements for participation of the Clients; and

(e) provide a copy of the Virtualization Assessment and Migration Planning Project Plan to the Province and at the same time provide written notification to the Province when the Virtualization Assessment and Migration Planning Project Plan Milestone (see table above) has been achieved.

10.2.2 Province Responsibilities

The Province will:

(a) communicate to the Clients information concerning the Virtualization Assessment and Migration Planning Project and describe the requirements for their participation; and

(b) obtain the participation of the Client in the Virtualization Assessment and Migration Planning Project.

10.3 Virtualization and Migration Test Lab

The Service Provider will establish a test lab at the At issue for Inquiry with hardware and software to support the Virtualization Assessment. This lab will be available to Service Provider Personnel for small scale proof-of-concept testing in connection with the Virtualization and Migration. For greater certainty, the test lab is not the test facility for the migration of the Province's Applications (and associated data).

The Service Provider will provide written notification to the Province when the Virtualization Assessment and Migration Test Lab Milestone (see table above) has been achieved (when it has been established at the

At issue for Inquiry

10.4 Virtualization Assessment and Migration Study

10.4.1 Service Provider Responsibilities

In this phase of the project, in accordance with the Virtualization Assessment and Migration Planning Project Plan, the Service Provider will:

(a) conduct an assessment of the Province Applications and data associated with the Province's current Server environment;

(b) with input from the Province, identify and consider the business drivers for scheduling the migration of individual Applications of the Clients including:

(i) Clients' requirements and Province freeze periods;

(ii) Operating System end of support timing (e.g. Windows 2000 in July 2010);

(iii) remaining Hardware amortization or service life;

(iv) desired STMS Data Centre;

(v) multi-application family constraints such as transaction or data access latency;

(vi) the impact of the Mainframe Services Migration on Clients' Applications that interact with Mainframe Applications or databases; and

(vii) the availability of the Province and Service Provider resources;

(c) in cooperation with the Technology Architecture Working Group, identify the technical criteria that must be considered in the determination of whether the target Server for each Application will be a Virtual Server or a Physical Server;

(d) deploy a data collection tool within the Province Network under the Change Management Procedures described in the Service Management SOW. The data collection tool may need to be installed in more than one location in the Province Network. The data collection tool will evaluate network traffic between servers and clients allowing the development of an "interdependency map". The data collection tool will not inhibit the Clients' operations or performance of their Applications in the Province Network and Server environment;

(e) consult with Clients to enable the Service Provider to identify the Applications operating on Servers within the Province's current Server environment and associated data and their business criticality;

(f) identify the data collection tool promptly following the Hand-Over Date. If the data collection tool requires the operation of scripts or Software Agents on the

Province Servers then such scripts or Software Agents will be implemented by the Service Provider in consultation with the Province and using the Change Management Procedures described in the Service Management SOW;

(g) develop and deliver to the Province:

(i) a reference architecture (the "**Reference Architecture**") document that details the proposed target architecture for the Applications and data of Clients that are associated with the Province Servers including application interdependencies, system performance criteria, network requirements, security requirements, storage requirements and backup/recovery requirements; and

(ii) a source to target document (the "**Source to Target Report**") that maps the Applications and data of Clients that are associated with the Province Servers to a proposed future Virtual and Physical Server environment; and

(h) provide written notification to the Province when Virtualization Assessment and Migration Study Milestone (see table above) has been achieved (when the Service Provider completes the Reference Architecture and Source to Target Report deliverables and provides copies thereof to the Province).

10.4.2 Province Responsibilities

The Province will:

(a) assist the Service Provider with the deployment of its data collection tool by making the required configuration changes to the Province Network including firewall and router changes; and

(b) facilitate the participation of Clients in this phase of the project.

10.5 Multi-Year Plan

In this phase of the project, in accordance with the findings of the Virtualization Assessment and Migration Study activities as described in Section 10.4 (*Virtualization Assessment and Migration Study*) above, the Service Provider and the Province will reach agreement on a Multi-Year Plan.

The Service Provider and the Province will develop an agreed to Multi-Year Plan based on and giving effect to the following planning assumptions agreed to by the Province and the Service Provider unless otherwise agreed to by the Province and the Service Provider pursuant to the Change Order Process:

(a) the Virtualization and Migration of the Province Server environment will take place by multiple overlapping virtualization and migration Waves each year during the first five years of the Agreement based on migrating Applications operating on the following approximate numbers of Servers and associated data:

(i) 10% of the Servers in Year 1 of the Agreement;

(ii) 20% of the Servers in Year 2 of the Agreement;

(iii) 30% of the Servers in Year 3 of the Agreement;

(iv) 20% of the Servers in Year 4 of the Agreement; and

(v) 20% of the Servers in Year 5 of the Agreement;

(b) there will be approximately 19 virtualization and migration Waves starting at approximately 3 month intervals as follows:

(i) during the early Waves, hardware refresh and virtualization will be performed "in-place" at the Province Data Centres;

(ii) when the STMS Data Centre in Calgary is operational, subsequent Waves will include the migration of Servers to the STMS Calgary Data Centre based upon: (A) the positioning of Servers to best enhance the disaster recovery capabilities of the Service Provider's solution; (B) the need to keep certain Servers located near the

At issue for Inquiry

(C) the VA commitment in each of the STMS Data Centres, unless application family performance constraints require transformation "in-place" at a Province Data Centre; and

(iii) when the STMS Interior Data Centre is operational subsequent Waves will be targeted to either STMS Data Centre;

(c) one of the approximately 19 virtualization and migration Waves will be planned to coincide with the Mainframe Services Migration in the event there are Applications and associated data that must migrate simultaneously with the Mainframe System;

(d) initial Waves will focus on lower complexity Applications and associated data. These Applications will require less effort and involve less risk in order to accelerate progress, refine the agreed procedures and build stakeholder confidence in the migration process through early successes; and

(e) when both STMS Data Centres are available, the Applications operating on Servers that have been transformed "in place" at the Province Data Centres and their associated data will be migrated in a separate series of "migration only" Waves to the STMS Data Centres as follows:

(i) there will also be approximately seven "migration-only" Waves;

(ii) Applications on Virtual Servers at the Province Data Centres will be migrated to another Virtual Server target environment at an STMS Data Centre;

(iii) Applications on Physical Servers at the Province Data Centres will be migrated to similar physical Servers at an STMS Data Centre; and

(iv) after migration, the Service Provider will move any of the Service Provider Servers displaced as a result of the "migration only" Waves from the Province Data Centres to the STMS Data Centres in preparation for subsequent migrations.

10.5.2 Additional Service Provider Responsibilities

The Service Provider will:

(a) based on the Reference Architecture, Source to Target Report and the business drivers identified in the previous phase, propose a draft Multi-Year Plan;

(b) consult with the Province to refine the draft Multi-Year Plan to reach agreement on the final Multi-Year Plan;

(c) cooperate with the Province to reach agreement on the final Multi-Year Plan in consultation with the Technology Architecture Working Group for review of design compliance with the Province's enterprise architecture and standards; and

(d) provide the Province with a copy of the Multi-Year Plan and at the same time provide written notification to the Province when the Virtualization Assessment and Migration Planning Project Plan Approved Milestone (see table above) has been achieved.

10.5.3 Province Responsibilities

The Province will:

(a) facilitate the participation of Clients to refine and reach agreement on the final Virtualization Assessment and Migration Planning Project Plan; and

(b) cooperate with the Service Provider to reach agreement on the final Multi-Year Plan in consultation with the Technology Architecture Working Group for review of design compliance with the Province's enterprise architecture and standards.

10.6 First Committed Annual Plan

The agreement of the Province and the Service Provider to the Multi-Year Plan will include the agreement of the Parties to the first 2 Waves described in the Multi-Year Plan (in order that detailed Wave planning can commence according to the Schedule in the Transformation Plan).

The first 2 Waves described in the Multi-Year Migration Plan will constitute the first Committed Annual Plan. The first 2 Waves will be deemed to be Committed Waves (as such term is defined in Section 15 (*Virtualization and Migration Project*) of this SOW) and will be completed as part

of the Virtualization and Migration Project described in Section 15 (*Virtualization and Migration Project*) of this SOW.

The Service Provider will provide written notification to the Province that the First Committed Annual Plan for August 2009-March 2010 (first 2 Virtualization and Migration Waves) Milestone (see table above) has been achieved when both Parties have agreed on the first 2 Waves described in the Multi-Year Plan.

10.6.1 Completion

For the purposes of this SOW, the Virtualization Assessment and Migration Planning for all Servers Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 10 (*Virtualization Assessment and Migration Planning Project*) have been achieved.

11. FIELD SERVICES

The purpose of the Field Services Transformation Project is to perform the activities necessary for the transfer of responsibility for the management of maintenance services and the performance of other related Field Services, as described in the On Site Services SOW, from the Province to the Service Provider on the Hand-Over Date.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Field Services Transformation	**Assumption of Responsibility**		N/A	Hand-Over Date	**Service Provider assumes responsibility on the Hand-Over Date**

11.1 Service Provider Field Services

11.1.1 Service Provider Responsibilities

The Service Provider will:

(a) on the Hand-Over Date, implement the escalation processes for provision of maintenance services and other related Field Services, as defined in the On Site Services SOW; and

(b) manage maintenance services and perform other related Field Services for the Managed Equipment located at the Remote Infrastructure Server Locations and Remote Application Server Locations as described in Schedule 8 (*Service Locations*), as described in the On Site Services SOW.

11.1.2 Province Responsibilities

The Province will:

(a) for each Province Server, maintain the maintenance service arrangements in place for such Server (such maintenance service arrangements do not include services provided to the Province by Navigata) until the Server is refreshed with a Service Provider Server; and

(b) provide the Service Provider with physical access to the Remote Sites as required in order to provide Field Services for the Managed Equipment managed by the Service Provider at such Remote Infrastructure Server Locations and Remote Application Server Locations.

11.1.3 Completion

For the purposes of this SOW, the Assumption of Responsibility Significant Milestones (see table above) will be deemed to be "complete" when the Service Provider has performed the activities necessary for the transfer of responsibility for the management of maintenance services and the performance of other related Field Services as described in Section 11 (*Field Services*).

12. STORAGE AND BACKUP

Pursuant to the Storage and Backup Transformation Project, the Service Provider will:

(a) add the Storage Management Tool Set of the Service Provider to the Service Provider's tool servers at the data centres utilized to provide Managed Storage Services and Managed Backup Services; and

(b) update the manuals for such services to reflect the utilization of the Storage Management Tool Set and any revised procedures implemented by the Service Provider in connection with such use.

The Storage Management Tool Set consists of EMC (EMC Command Console) enabling the Service Provider to monitor and manage storage devices at data centres.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation

(Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Storage and Backup Transformation Project	**Install Service Provider Storage Management and Backup Management Tools at Province Data Centres**	Configure Management Tool Sets at Province Data Centres	See Schedule 23 (*Fees*), Appendix I	Month 5, August, 2009	**Service Provider processes for managing storage services and backup services are implemented**
		Develop Managed Storage and Managed Backup Sections of the Manual	See Schedule 23 (*Fees*), Appendix I	Month 5, August, 2009	
	Install Service Provider Storage Management and Backup Management Tools at the STMS Calgary Data Centre	Update Managed Storage and Managed Backup Sections of the Manual	See Schedule 23 (*Fees*), Appendix I	Month 7, October, 2009	**STMS Calgary Data Centre Storage and Backup Services ready for application and data migration**
		Configure Management Tool Sets for STMS Calgary Data Centre	See Schedule 23 (*Fees*), Appendix I	Month 9, December, 2009	
	Install Service Provider Storage Management and Backup Management Tools at the STMS Interior Data Centre	Update Managed Storage and Managed Backup Sections of the Manual	See Schedule 23 (*Fees*), Appendix I	Month 24, March, 2011	**STMS Interior Data Centre Storage and Backup Services ready for application and data migration** **Ready for site to site back ups**
		Configure Management Tool Sets for STMS Interior Data Centre	See Schedule 23 (*Fees*), Appendix I	Month 26, May, 2011	

12.2 Province Data Centres

12.2.1 Configure Management Tools

The Service Provider will install and configure the Storage Management Tool Set on tool Servers of the Service Provider at the Province Data Centres S. 15 S. 15 as described in Section 9.2.4 (*Storage Management Tools*).

The Service Provider will provide written notification to the Province when the Configure Management Tool Sets at Province Data Centres Milestone (see table above) has been achieved (when the Storage Management Tool Set has been installed and configured at the Province Data Centres).

12.2.2 Manual for Managed Storage and Managed Backup

The Managed Storage and Managed Backup sections of the Manual set out the specific operating procedures, processes, tasks and functions that are required to be performed by the Service Provider to deliver the Managed Storage Services and Managed Backup Services.

At the Hand-Over Date, the Service Provider will utilize the Province's existing manual for the Managed Storage and Managed Backup Services.

The Service Provider will develop the Managed Storage and Managed Backup sections of the Manual in accordance with the Agreement, based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*) and as the Province procedures are revised in connection with the implementation of the Service Provider's operating procedures.

The Service Provider will provide written notification to the Province when the Develop Managed Storage and Managed Backup Sections of the Manual Milestone (see table above) has been achieved (when the Managed Storage and Managed Backup sections of the Manual describe the Managed Storage Services and Managed Backup Services being provided by the Service Provider from the Province Data Centres at S. 15 in accordance with the requirements of the Agreement).

12.2.3 Completion

For the purposes of this SOW, the Install Service Provider Storage Management and Backup Management Tools at Province Data Centres Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Sections 12.2 (*Province Data Centres*) have been achieved.

12.3 STMS Calgary Data Centre

The Service Provider will also utilize the Storage Management and Backup Management Tool Sets to monitor and manage storage and backup devices at the STMS Calgary Data Centre.

The Service Provider will:

(a) install and configure the Storage Management and Backup Management Tool Sets on the tool Servers of the Service Provider that were installed at the STMS Calgary Data Centre under Section 9.6 (*Install Standard Tools at STMS Data Centres*) of this SOW;

(b) update the Managed Storage and Managed Backup section of the Manual, in accordance with the Agreement and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*), to reflect the provision of Managed Storage Services and Managed Backup Services from the STMS Calgary Data Centre; and

(c) provide written notification to the Province when the Configure Management Tool Sets for STMS Calgary Data Centre and the Update Managed Storage and

Managed Backup Sections of the Manual Milestones (see table above) have been achieved (when its Storage Management and Backup Management Tool Sets have been installed and configured at the STMS Calgary Data Centre and the Managed Storage and Managed Backup section of the Manual has been updated).

12.3.2 Completion

For the purposes of this SOW, the Install Service Provider Storage Management and Backup Management Tools at the STMS Calgary Data Centre Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 12.3 (*STMS Calgary Data Centre*) have been achieved.

12.4 STMS Interior Data Centre

The Service Provider will also utilize the Storage Management and Backup Management Tool Sets to monitor and manage storage and backup devices at the STMS Interior Data Centre.

The Service Provider will:

(a) install and configure the Storage Management and Backup Management Tool Sets on the tool Servers of the Service Provider that were installed at the STMS Interior Data Centre under Section 9.6 (*Install Standard Tools at STMS Data Centres*) of this SOW;

(b) test site to site data replication between the STMS Interior Data Centre and the STMS Calgary Data Centre;

(c) update the Managed Storage and Managed Backup section of the Manual, in accordance with the Agreement and based on the Manual Outline attached to this SOW as Appendix C (*Manual Outline*), to reflect the provision of Managed Storage Services and Managed Backup Services from the STMS Interior Data Centre; and

(d) provide written notification to the Province when the Configure Management Tool Sets for STMS Interior Data Centre and the Update Managed Storage and Managed Backup Sections of the Manual Milestone (see table above) have been achieved (when its Storage Management and Backup Management Tool Sets have been installed and configured at the STMS Interior Data Centre and the Managed Storage and Managed Backup section of the Manual has been updated).

12.4.2 Completion

For the purposes of this SOW, the Install Service Provider Storage Management and Backup Management Tools at the STMS Interior Data Centre Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 12.4 (*STMS Interior Data Centre*) have been achieved.

13. AFTER HOURS SERVICE DESK (OPTIONAL SERVICES)

If the Province elects to proceed with this optional After Hours Service Desk Transformation Project, the Service Provider will assume responsibility for after hours service desk coverage from 7:00 PM to 7:00 AM Pacific Time on Business Days and 24 hour coverage on non-Business Days.

The Province will continue to operate the Service Desk during Business Days from 7:00 AM to 7:00 PM Pacific Time.

There shall be no charge to the Province for the After Hours Service Desk Transformation Project other than the ongoing operational costs.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
After Hours Service Desk Transformation	**Process Integration Activities**	Process Integration Activities	See Schedule 23 (*Fees*), Appendix I	Month 3, June, 2009	**After hours service desk function transferred to Service Provider**
	Add STMS After Hours Service Desk Services to Existing Service Provider Service Desk	After Hours Service Desk Go Live	See Schedule 23 (*Fees*), Appendix I	Month 4, July, 2009 (date to be confirmed)	

13.1 Process Integration Activities

13.1.1 Service Provider Responsibilities

The Service Provider will:

(a) train its staff on the required after hours service desk processes and on the use of the Province's Service Desk Tool;

(b) test connectivity from the Service Provider's Service Location via the internet to the Province's Service Desk Tool hosted in the Province's Desktop Terminal Services (DTS) Citrix environment;

(c) configure and test the Service Provider's Automated Call Distribution tool;

(d) perform end to end testing through the use of simulated calls; and

(e) provide written notification to the Province when the Process Integration Activities Milestone (see table above) has been achieved (when the staff has been trained, connectivity has been tested and readiness of the Service Provider has been approved by the Province).

13.1.2 Province Responsibilities

The Province will:

(a) provide documentation on the required after hours service desk processes and use of their Service Desk Tool;

(b) provide "train the trainer" training to the Service Provider on the required after hours service desk processes and on the use of the Province's Service Desk Tool;

(c) provide access to the Province's Service Desk Tool testing environment;

(d) support the Service Providers end to end testing by providing test call scenarios and instructing the Service Provider how to record the test call scenarios in the Province's test Service Desk Tool; and

(e) following successful completion of end to end testing, approve the readiness of the Service Provider to provide the after hours service desk services.

13.1.3 Completion

For the purposes of this SOW, the Process Integration Activities Significant Milestones (see table above) will be deemed to be "complete" when the milestone in Section 13.1 (*Process Integration Activities*) has been achieved.

13.2 After Hours Service Desk Go Live

13.2.1 Service Provider Responsibilities

The Service Provider will:

(a) begin to provide the after hours service desk services at the Effective Time; and

(b) provide written notification to the Province when the After Hours Service Desk Go Live Milestone (see table above) has been achieved (when the Service Provider is providing the after hours service desk services).

13.2.2 Province Responsibilities

The Province will:

(a) cause the redirection of the existing after hours service desk access phone numbers to the Service Provider at the Effective Time;

(b) provide the Service Provider with access to the Province Service Desk Tool hosted in the Province's Desktop Terminal Services (DTS) Citrix environment;

(c) decommission any Province procedures associated with existing after hours service desk Service Provider; and

(d) decommission its existing after hours service desk after the Effective Time.

13.2.3 Completion

For the purposes of this SOW, the Add STMS After Hours Service Desk Services to Existing Service Provider Service Desk Significant Milestones (see table above) will be deemed to be "complete" when the milestone in Section 13.2 (*After Hours Service Desk Go Live*) has been achieved.

14. SECURITY TRANSFORMATION

The Security Transformation Project involves the following projects as described in this section:

- perform Initial Security Policy Compliance Scan;
- perform Initial Anti-Virus Scan;
- perform Security Threat and Risk Assessments and Privacy Impact Assessments;
- perform Privileged ID Management Improvement; and
- Additional Services:
    - Security Information Management / Enterprise Security Event Project;
    - Payment Card Industry Data Security Standard Compliant Infrastructure Project;
    - Two Factor Authentication Project for Service Provider Privileged Access; and
    - Two Factor Authentication Project for Province Privileged Access.

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that

such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Security Transformation	**Virus Scan (described in Service Systems Management section)**	Initial Anti-Virus Scan for existing Province servers	N/A	Month 4, July, 2009	**Service Provider reports to Province on results and remediates any viruses found**
	Security Compliance Scan (described in Server Systems Management section)	Initial Security Policy Compliance Scan on servers	N/A	Month 6, September, 2009	**Service Provider reports to Province on security compliance findings**
	Security Threat and Risk Assessments and Privacy Impact Assessments	As required in each Transformation Project	N/A	Dates and applicability to be determined by Month 3, June, 2009 and documented in the Revised Transformation Plan	**As defined in Schedules 18 or 24**

S. 15

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
	Additional Services	Security Information Management / Enterprise Security Event Project	See Schedule 23 (*Fees*), Appendix I S. 15	To be determined when service is ordered by the Province	**Subject to optional security services being funded by the Province for greater security** S. 15

14.1 Perform Initial Security Policy Compliance Scan

The Service Provider will complete the initial Security Policy Compliance Scan pursuant to Section 9.5 (*Perform Initial Security Policy Compliance Scan*) of this SOW.

14.2 Perform Initial Anti-Virus Scan

The Service Provider will complete the initial Anti-Virus Scan pursuant to Section 9.4 (*Perform Initial Anti-Virus Scan*) of this SOW.

14.3 Security Threat and Risk Assessments and Privacy Impact Assessments

The Service Provider will conduct Security Threat and Risk Assessments (STRA) in respect of the Transformation Projects as required pursuant to Schedule 24 (*Privacy Obligations*). The Parties will document, in the Revised Transformation Plan, such other STRAs as are required in respect of the Transformation Projects pursuant to Schedule 24 (*Privacy Obligations*).

The Province will conduct Privacy Impact Assessments (PIA) with support from the Service Provider in respect of the Transformation Projects as required pursuant to Schedule 24 (*Privacy Obligations*). The Parties will document, in the Revised Transformation Plan, the PIAs required in respect of the Transformation Projects pursuant to Schedule 24 (*Privacy Obligations*).

The Service Provider will provide written notification to the Province when the Security Threat and Risk Assessments and Privacy Impact Assessments have been achieved (when the Security Threat and Risk Assessments and Privacy Impact Assessment are completed as documented in each Transformation Project and the Revised Transformation Plan).

14.3.1 Completion

For the purposes of this SOW, the Security Threat and Risk Assessments and Privacy Impact Assessments will be deemed to be "complete" when all of the Security Threat and Risk Assessments and the Privacy Impact Assessments documented in each Transformation Project and the Revised Transformation Plan have been completed.

14.4 S. 15

S. 15

S. 15 The Parties will review such plan in accordance with the Governance Process and implement it to the extent agreed pursuant to the Change Order Process.

14.4.1 Additional Service Provider Responsibilities

The Service Provider will:

(a) from the Hand Over Date, manage S. 15 of the Service Provider Personnel;

(b) monitor, with the Software tools available to the Service Provider, S. 15 S. 15 by Service Provider Personnel and Province Staff;

(c) propose to the Province, in accordance with the Change Order Process, additional tools to enhance the Service Provider's ability, in cooperation with the Province, to: (i) S. 15 by Service Provider Personnel and Province Staff; and (ii) S. 15

S. 15

(d) make recommendations to the Province on an ongoing basis on additional measures that may be implemented to reduce the number of Privileged IDs based on the need-to-know and least privilege principles;

(e) assess, in connection with the performance of its root cause analysis of Problems,

S. 15

(f) report to the Province the number of Problems in which S. 15 S. 15 S. 15 after the Hand-Over Date;

(g) report to the Province any change in the number of S. 15 S. 15 review with the Province the progress of the Parties in reducing the number of S. 15 S. 15 after the Hand-Over Date; and

(h) develop in cooperation with the Province a procedure that, when implemented, will provide advance notice to the Service Provider S. 15 S. 15

14.4.2 Province Responsibilities

The Province will:

(a) continue to manage S. 15 of the Province Staff;

(b) manage the Province's S. 15 S. 15

(c) review the Province's policies and procedures S. 15 S. 15

(d) review, for acceptability, Change Requests submitted by the Service Provider for the implementation of additional monitoring tools S. 15 S. 15

(e) review, for acceptability, recommendations from the Service Provider on additional measures that may be implemented S. 15 S. 15 ; and

(f) cooperate with the Service Provider in the development and implementation of a procedure to provide advance notice to the Service Provider of S. 15 S. 15

14.4.3 Completion

For the purposes of this SOW, S. 15 Significant Milestones (see table above) will be deemed to be "complete" when all of the milestones in Section 14.4 S. 15 have been achieved as described in the Revised Transformation Plan.

14.5 Additional Services

This section refers to Additional Services that may be acquired, at the option of the Province, as described in the Security SOW pursuant to the Change Order Process.

14.5.1 Security Information Management / Enterprise Security Event Project

Further to this project, the Parties will establish the infrastructure and Security Operations Centre (SOC) to support the Enterprise Security Event Management (ESEM) Services as described in Section 8.1 of the Security SOW.

14.5.1.1 Service Provider Responsibilities

In accordance with the Change Order implementing this project, the Service Provider will:

(a) develop a detailed implementation plan in consultation with the Province including requirements for Province participation;

(b) procure, prepare, and install hardware, software, or third party services as required by the Security SOW and specified in the detailed implementation plan;

(c) establish the SOC facility;

(d) implement the Service Provider staffing plan, training and operational procedures;

(e) work with the Province to define test cases and acceptance test criteria for the implementation of the ESEM Services;

(f) design the required network access for the operation of the ESEM Services including firewall and router changes;

(g) conduct the agreed to testing in cooperation with the Province;

(h) upon completion of the implementation and testing activities including achievement of all acceptance test criteria, provide notice to the Province that the Security Information Management/Enterprise Security Event Project Milestone (see table above) has been achieved when it is ready to commence delivery of the ESEM Services; and

(i) upon approval of the Province for commencement of the ESEM Services, begin to deliver the ESEM Services as described in the Security SOW.

14.5.1.2 Province Responsibilities

In accordance with the Change Order implementing this project, the Province will:

(a) facilitate the required Province participation as agreed with the Service Provider in the detailed implementation plan;

(b) work with the Service Provider to define test cases and acceptance test criteria for the implementation of the ESEM Services;

(c) implement the required network access for operation of the ESEM Services including firewall and router changes; and

(d) participate in the agreed to testing in cooperation with the Service Provider.

14.5.1.3 Completion

For the purposes of this SOW, the Security Information Management / Enterprise Security Event Project Milestone (see table above) will be deemed to be "complete" when all the milestones within the detailed implementation plan have been achieved as per the detailed implementation plan prepared by the Parties as described in Section 14.5.1 (*Security Information Management/Enterprise Security Event Project*).

14.5.2 Payment Card Industry Data Security Standard Compliant Infrastructure Project

Further to this project, the Parties will establish the infrastructure and services required to support the Payment Card Industry Data Security Standard Compliant Infrastructure Project (PCI/DSS) as described in Section 8.3 of the Security SOW.

14.5.2.1 Service Provider Responsibilities

In accordance with the Change Order implementing this project, the Service Provider will:

(a) develop a detailed implementation plan in consultation with the Province including requirements for Province participation;

(b) procure, prepare, and install hardware, software, or third party services as required by the Security SOW and specified in the detailed implementation plan;

(c) establish a production PCI compartment (the "**Production PCI Compartment**") at one of the STMS Data Centres;

(d) establish a development and testing PCI compartment at the other STMS Data Centre which will also be used for Disaster Recovery purposes;

(e) work with the Province to identify Applications and servers that are required to be migrated to the PCI compartment;

(f) document and test all ongoing operational processes (network and server log monitoring and review, and vulnerability testing);

(g) document all operational hosting procedures as required for PCI compliance;

(h) work with the Province to define test cases and acceptance test criteria for the implementation of the PCI/DSS Services;

(i) complete the Qualified Security Assessor (QSA) review and certification of environment as outlined in the Security SOW;

(j) establish a Disaster Recovery Plan to allow the production PCI facility to be recovered in the development and testing PCI compartment;

(k) design and implement required network access for the operation of the PCI/DSS Services including firewall and router changes;

(l) conduct the agreed to testing in cooperation with the Province;

(m) upon successful testing, migrate the in scope application and servers to the PCI compartment;

(n) upon completion of the implementation and testing activities including achievement of all acceptance test criteria, provide notice to the Province that the Payment Card Industry Data Security Standard Compliant Infrastructure Project Milestone (see table above) has been achieved when it is ready to commence delivery of the PCI/DSS Services; and

(o) upon approval of the Province for commencement of the PCI/DSS Services, migrate the in-scope Applications and servers to the Production PCI Compartment and begin to deliver the PCI/DSS Services as described in the Security SOW.

14.5.2.2 Province Responsibilities

In accordance with the Change Order implementing this project, the Province will:

(a) facilitate the required Province participation as agreed with the Service Provider in the detailed implementation plan;

(b) work with the Service Provider to define test cases and acceptance test criteria for the implementation of the PCI/DSS Services;

(c) assist the Service Provider with the implementation of the PCI/DSS Services by identifying the required firewall rules and router changes to allow the appropriate communication required for the application to function as intended;

(d) identify the authorized application administrators who will require access to the PCI compartment using Two Factor Authentication;

(e) participate in the agreed to testing in cooperation with the Service Provider; and

(f) upon successful test, authorize the migration of the in-scope Applications and servers to the Production PCI Compartment.

14.5.2.3 Completion

For the purposes of this SOW, the Payment Card Industry Data Security Standard Compliant Infrastructure Project Milestone (see table above) will be deemed to be "complete" when all the milestones within the detailed implementation plan have been achieved as per the detailed implementation plan prepared by the Parties as described in Section 14.5.2 (*Payment Card Industry Data Security Standard Compliant Infrastructure Project*).

14.5.3 Two Factor Authentication Project for Service Provider Privileged Access

Further to this project, the Service Provider will establish the infrastructure to support the Two Factor Authentication (2FA) Project for Service Provider Privileged Access as described in Section 8.1 of the Security SOW.

In accordance with the Change Order implementing this project, the Service Provider will:

(a) develop a detailed implementation plan in consultation with the Province;

(b) procure, prepare, and install hardware, software, or third party services as required by the Security SOW and specified in the detailed implementation plan;

(c) work with the Province to define test cases and acceptance test criteria for the implementation of the 2FA Project for Service Provider Privileged Access;

(d) manage allocation of Fobs to the authorized Service Provider administrative staff;

(e) conduct the agreed to testing in cooperation with the Province; and

(f) upon completion of the implementation and testing activities including achievement of all acceptance test criteria, provide notice to the Province that the Two Factor Authentication Project for Service Provider Privileged Access Milestone (see table above) has been achieved when it is ready to commence delivery of the 2FA Project for Service Provider Privileged Access.

14.5.3.2 Completion

For the purposes of this SOW, the Two Factor Authentication Project for Service Provider Privileged Access Project Milestone (see table above) will be deemed to be "complete" when all the milestones within the detailed implementation plan have been achieved as per the detailed implementation plan prepared by the Parties as described in Section 14.5.3 (*Two Factor Authentication Project for Service Provider Privileged Access*).

14.5.4 Two Factor Authentication Project for Province Privileged Access

Further to this project, the Parties will establish the infrastructure to support the Citrix Secure Access Gateway (SAG) and the Two Factor Authentication (2FA) services for Province Staff's privileged access as described in Sections 8.1 and 8.2 of the Security SOW.

14.5.4.1 Service Provider Responsibilities

In accordance with the Change Order implementing this project, the Service Provider will:

(a) develop a detailed implementation plan in consultation with the Province including requirements for Province participation;

(b) procure, prepare, and install hardware, software, and third party services as required by the Security SOW and specified in the detailed implementation plan;

(c) install the application administration tools identified and provided by the Province that are required to be hosted within the Citrix Secure Access Gateway;

(d) work with the Province to define test cases and acceptance test criteria for the implementation of the Citrix Secure Access Gateway services and the Two Factor Authentications services for Province Staff's privileged access;

(e) design required network access for the operation of the Citrix Secure Access Gateway services and Two Factor Authentication services for Province Staff's privileged access;

(f) execute the agreed to testing in cooperation with the Province; and

(g) upon completion of the implementation and testing activities including achievement of all acceptance test criteria, provide notice to the Province that the Two Factor Authentication Project for Province Privileged Access Milestone (see table above) has been achieved when it is ready to commence delivery of the Citrix Secure Access Gateway services and the Two Factor Authentication services for Province Staff's privileged access.

14.5.4.2 Province Responsibilities

In accordance with the Change Order implementing this project, the Province will:

(a) facilitate the required Province participation as agreed with the Service Provider in the detailed implementation plan;

(b) establish procedures for the administration and S. 15 S. 15 to Province Staff;

(c) identify and provide the application administration tools that the Province requires to be hosted within the Citrix Secure Access Gateway;

(d) work with the Service Provider to define test cases and acceptance test criteria for the implementation of the Citrix Secure Access Gateway services and the Two Factor Authentication services for Province Staff's privileged access;

(e) assist the Service Provider with the implementation of the Citrix Secure Access Gateway services and the Two Factor Authentication services for Province Staff's privileged access by making the required configuration changes to the Province's network including firewall and router changes;

(f) participate in the agreed to testing in cooperation with the Service Provider; and

(g) upon approval of the Province for commencement of the Citrix Secure Access Gateway services and the Two Factor Authentication services for Province Staff's privileged access, begin to manage and utilize the Citrix Secure Access Gateway services and the Two Factor Authentication services for Province Staff's privileged access as described in the Security SOW.

14.5.4.3 Completion

For the purposes of this SOW, the Two Factor Authentication Project for Province Privileged Access Project Milestone (see table above) will be deemed to be "complete" when all the milestones within the detailed implementation plan have been achieved as per the detailed implementation plan prepared by the Parties as described in Section 14.5.3 (*Two Factor Authentication Project for Service Provider Privileged Access*).

15. VIRTUALIZATION AND MIGRATION PROJECT

The Virtualization and Migration Transformation Project provides for the migration of Servers (Applications and associated data) to the STMS Data Centres (the "**Migration**") with Virtualization of Servers to the extent agreed in the Multi-Year Plan approved by the Parties. The Service Provider and the Province will develop a Multi-Year Plan for Virtualization and Migration of Applications to the STMS Data Centres under the Virtualization and Migration Planning Project described in Section 10 (*Virtualization Assessment and Migration Planning Project*) of this SOW. The Multi-Year Plan will be comprised of five annual plans (each an "**Annual Plan**"). Under the Multi-Year Plan, each of the Applications to be Migrated, and if agreed Virtualized, will be assigned to a specific Wave within one of the Annual Plans.

After the Multi-Year Plan for the Virtualization and Migration Project has been approved by the Parties, it will be implemented in Committed Waves in accordance with the Committed Annual Plans agreed to by the Province and the Service Provider as contemplated in Section 15.1 (*Committed Annual Plans*) of this SOW.

There are four types of Waves that will be implemented under the Committed Annual Plans:

- Typical virtualization and migration Waves (Section 15.3);
- Mainframe Services Migration Wave (Section 15.4);
- "Migration-only" Waves (Section 15.5); and
- Migration of "unrefreshable Servers" Wave (Section 15.6).

The table below sets forth the name of the Transformation Project (Column 1), each significant milestone to be achieved by the Service Provider under such Transformation Project (Column 2), all milestones to be achieved by the Service Provider that have an associated payment obligation (Column 3) and the price therefor (Column 4), the date that such milestone must be completed or achieved by the Service Provider (Column 5) and the acceptance criteria or the criteria that must be met for a milestone to be considered completed or achieved.

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
Virtualization and Migration Project	**Approximately 27 Migration Waves to transfer all Province non-Mainframe Applications and their related data to the STMS Data Centres with Virtualization of Servers to the extent possible.**	Midrange support for Waves from first Committed Annual Plan	See Schedule 23 (*Fees*), Appendix I	Month 5-12, August, 2009 - March, 2010	**All Applications migrated with no loss of data integrity.** **Completion of the Second Committed Annual Plan – Fifth Committed Annual Plan**
		Storage support for Waves from first Committed Annual Plan		Month 5-12, August, 2009 - March, 2010	
		Network support for Waves from first Committed Annual Plan		Month 5-12, August, 2009 - March, 2010	
		Second Committed Annual Plan for year-ending March 2011 (4 Virtualization and Migration Waves plus Mainframe Wave)		Month 9, December, 2009	
		Midrange support for Waves from second Committed Annual Plan		Month 10-24, January, 2010 - March, 2011	
		Storage support for Waves from second Committed Annual Plan		Month 10-24, January, 2010 - March, 2011	
		Network support for Waves from		Month 10-24, January,	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
		second Committed Annual Plan		2010 - March, 2011	
		Third Committed Annual Plan for year-ending March 2012 (4 Virtualization and Migration Waves)		Month 21, December, 2010	
		Midrange support for Waves from third Committed Annual Plan		Month 22-36, January, 2011 - March, 2012	
		Storage support for Waves from third Committed Annual Plan		Month 22-36, January, 2011 - March, 2012	
		Network support for Waves from third Committed Annual Plan		Month 22-36, January, 2011 - March, 2012	
		Fourth Committed Annual Plan for year-ending March 2013 (4 Virtualization and Migration Waves and 4 "Migration-only" Waves)		Month 33, December, 2011	
		Midrange support for Waves from fourth Committed Annual Plan		Month 34-48, January, 2012 - March, 2013	
		Storage support for Waves from fourth Committed		Month 34-48, January, 2012 - March,	

Transformation Project	Significant Milestones (see table above)	Payment Milestones (see table above) (if applicable)	Price	Date of Deliverable	Acceptance Criteria
		Annual Plan		2013	
		Network support for Waves from fourth Committed Annual Plan		Month 34-48, January, 2012 - March, 2013	
		Fifth Committed Annual Plan for year-ending March 2014 (4 Virtualization and Migration Waves, 3 "Migration-only" Waves and the "unrefreshable" Servers)		Month 45, December, 2012	
		Midrange support for Waves from fifth Committed Annual Plan		Month 46-60, January, 2013 - March, 2014	
		Storage support for Waves from fifth Committed Annual Plan		Month 46-60, January, 2013 - March, 2014	
		Network support for Waves from fifth Committed Annual Plan		Month 46-60, January, 2013 - March, 2014	

15.1 Committed Annual Plans

The Parties will implement the Multi-Year Plan for the Virtualization and Migration Project in Waves, in accordance with five committed annual plans ("**Committed Annual Plans**") agreed to by the Province and the Service Provider. Section 15.1.1 (*Committed Annual Plans and Committed Waves*) sets out the process under which the Province and the Service Provider will agree to Committed Annual Plans and the Migration of Applications in Waves to Physical Servers or Virtual Servers under the Committed Annual Plans. Section 15.1.2 (*Adjustments*) sets out the agreements of the Province and the Service Provider with respect to adjustments to the

Virtualization and Migration Project, to Committed Annual Plans and to the Waves under which Applications are to be migrated to Physical Servers or Virtual Servers.

15.1.1 Committed Annual Plans and Committed Waves

The Parties will implement the Multi-Year Plan for the Virtualization and Migration Project in Waves, in accordance with five Committed Annual Plans agreed to by the Province and the Service Provider as follows:

(a) each Committed Annual Plan will include all Waves planned for a Contract Year (other than in respect of the first Committed Annual Plan which will be only a portion of a Contract Year and will include two Waves) and will be agreed to by the Parties no less than six months prior to the beginning of the Contract Year;

(b) the preparation for the first Wave of each Committed Annual Plan will commence 3 months before the beginning of that Contract Year as illustrated in the Transformation Plan;

(c) the Committed Annual Plan will set out the schedule for each of the Waves within such Committed Annual Plan including the time frames for all phases of each of the Waves;

(d) the Province may adjust the specific Servers included in each Wave provided that the required percentage of Servers for Virtualization and Migration in Contract Years 1 – 5, as set forth in Section 10.4(a) (*Multi-Year Plan*) above, is met;

(e) it is the intention of the parties that each Committed Wave in a Committed Annual Plan will require approximately the same level of effort by the Service Provider to complete; and

(f) no less than three months prior to the commencement of each Wave within a Committed Annual Plan, the Province will identify and confirm, to the Service Provider, the specific Servers (Applications) that shall be included in such Wave (each a "**Committed Wave**") and whether such Servers will be migrated to a Physical Server or a Virtual Server (for greater certainty, once the Province has confirmed the specific Servers (Applications) that will be included in a Wave as set out in this paragraph, there will be no adjustments to the Servers (Applications) that are being migrated or the Servers (Applications) that are being Migrated and Virtualized in the Wave except as may be agreed by the Parties.

The Service Provider will complete the Virtualization and Migration of Servers in accordance with the Committed Annual Plans and Committed Waves.

The Province will facilitate the participation of Clients in the Virtualization and Migration Project and the performance of the Clients' responsibilities relating thereto such that the Clients' Applications are Migrated and Virtualized as contemplated under the Committed Annual Plans and Committed Waves agreed to by the Parties.

The Service Provider will provide the Joint Operating Committee with monthly reports on the progress of the Virtualization and Migration Project under each Committed Annual Plan and Committed Wave. Where the reporting provided by the Service Provider indicates that the Virtualization and Migration Project is behind schedule, the Parties will cooperate to identify and implement any actions that can be undertaken to accelerate Virtualization and Migration with a view to getting the project back on schedule.

By way of example only, the table below illustrates the key dates for each Wave of the Third Committed Annual Plan (for the third Contract Year) where such dates are determined in accordance with this Section 15.1.1 (*Committed Annual Plans and Committed Waves*).

CAP Agreed (6 months prior to Contract Year)	Wave	Committed Wave Agreed and Start of Detail Planning	Target Environment Ready	Testing and Migration Start	Testing and Migration End
01-Oct-2010	1	01-Jan-2011	31-Mar-2011	01-Apr-2011	30-Jun-2011
01-Oct-2010	2	01-Apr-2011	30-Jun-2011	01-Jul-2011	30-Sep-2011
01-Oct-2010	3	01-Jul-2011	30-Sep-2011	01-Oct-2011	31-Dec-2011
01-Oct-2010	4	01-Oct-2011	31-Dec-2011	01-Jan-2012	31-Mar-2012

15.1.2 Adjustments

This Section 15.1.2 (*Adjustments*) sets out the agreement of the Parties with respect to adjustments to the Virtualization and Migration Project, to Committed Annual Plans and to Committed Waves.

In this section, "**Shortfall**" in respect of any Contract Year means the difference between the number of Servers contemplated to be Migrated to Physical Servers or Virtual Servers under the Annual Plan for such Contract Year forming part of the Multi-Year Plan and the number of Servers actually Migrated to Physical Servers or Virtual Servers in such Contract Year.

The Province and the Service Provider agree as follows:

(a) if a Server is to be Migrated to a Physical Server or Virtual Server in a Committed Wave and the Server is withdrawn from the Migration at the request of the Province, then the Service Provider will make reasonable efforts: (1) to adjust the Committed Wave by substituting another Server for the Server that has been withdrawn; and (2) if requested, to insert the Application that has been withdrawn into such subsequent Wave as is requested by the Province to the extent that such adjustments can be reasonably accommodated by the Service Provider;

(b) if, at the end of any Contract Year, there is a Shortfall in the number of Servers that have been Migrated to Physical Servers or Virtual Servers as a result of the action or failure to act of the Province (including the failure of the Province to include in any Committed Wave the number of Servers to be included thereunder

in accordance with Section 15.1.1 (*Committed Annual Plans and Committed Waves*) or the withdrawal by the Province from a Committed Wave), then:

(i) the Service Provider shall make reasonable efforts, to compensate for the Shortfall by including additional Servers (Applications) in subsequent Waves where requested to do so by the Province;

(ii) if the Shortfall at the end of a Contract Year is greater than or equal to the number set out in Table 15.1 – Shortfall below for the Contract Year, and the Service Provider's costs for completing the Virtualization and Migration Project will increase as a result thereof, then the Service Provider will be entitled to a Change Order in respect of such increased costs.

Table 15.1 - Shortfall

End of Contract Year	Shortfall
1	90
2	70
3	40
4	20

For greater certainty, the Service Provider will not be entitled to a Change Order to the extent that the Shortfall is attributable to the actions or failure to act of the Service Provider; and

(c) if: (i) the Multi-Year Plan will not be completed in the first five years of the Term (prior to March 31, 2014); (ii) the failure to complete the Multi-Year Plan within the first five years of the Term is attributable to the failure of the Province to perform its obligations relating to the Migration (including obligations relating to Virtualization where applicable); and (iii) the Service Provider's costs for completing the Virtualization and Migration Project under the Multi-Year Plan will increase as a result thereof; then the Service Provider will be entitled to a Change Order in respect of such increased costs under the Change Order Process.

If the Service Provider is entitled to a Change Order under the circumstances contemplated in paragraphs (b) – (c) above, the Service Provider will not be required to wait until the Virtualization and Migration Project is completed before submitting the Change Request in respect thereof. The Service Provider may submit the Change Request at such time as the Service Provider is able to substantiate that the conditions required for the Change Order have been satisfied and the Parties will process the Change Request in accordance with the Change Order Process.

Subject to the foregoing, if the Virtualization and Migration Project:

(d) is completed within two months of the completion date for the Virtualization and Migration Project set out in the Multi-Year Plan first agreed to by the Parties, then each of the Parties will bear any costs that may be incurred by it due to any delay beyond the originally scheduled completion date and neither Party will make a Claim of any nature whatsoever against the other Party in respect of the delay in the implementation of the project; and

(e) is not completed within two months of the completion date for the Virtualization and Migration Project set out in the Multi-Year Plan first agreed to by the Parties, then either Party can make a Claim against the other for any costs incurred by such Party in respect of the delay that are attributable to the act or neglect of the other Party.

15.2 Migration Waves

The Parties will implement the Virtualization and Migration Transformation Project in accordance with the Committed Annual Plans in Waves. There are four types of Waves, each of which includes the following phases:

(a) detailed planning and design of each Wave in consultation with the Province Alliance Management Office and Client stakeholders;

(b) procurement, installation and configuration of required hardware and software;

(c) Virtualization and Migration testing;

(d) Virtualization and Migration pilot; and

(e) Virtualization and Migration with a fallback contingency plan in the event of failure.

The four types of Waves are described in more detail in Sections 15.3 to 15.6 inclusive below.

15.3 Plan of a Typical Virtualization and Migration Wave

The lifecycle of a typical virtualization and migration Wave is expected to be at least six months. The typical virtualization and migration Wave involves the following steps:

(a) detailed Engineering Design and Plan for the Wave;

(b) hardware and software order;

(c) hardware and software installation and configuration;

(d) Virtualization and Migration tests for each application in the Wave to verify the virtualization and migration plan, performance of the application and successful

integration of any necessary application or other changes in the Province's environment;

(e) Virtualization and Migration pilot tests for each application in the Wave to verify network configuration changes, test the data migration process, confirm timing for the migration, and test the fallback contingency plans; and

(f) Virtualization and Migration of each application with a fallback contingency plan in case of failure.

15.3.2 Detailed Engineering Design and Plan

15.3.2.1 Service Provider Responsibilities

The Service Provider will:

(a) develop the detailed engineering plans and proposed task schedule for the virtualization and migration Wave (the "**Wave Plan**") taking into account any virtualization contemplated for the Wave in the Multi-Year Plan;

(b) propose a schedule for physical and virtual Server installation, application and data migration testing and the virtualization and migration;

(c) create, as part of the Wave Plan, a detailed project plan in consultation with Clients;

(d) identify and finalize LAN requirements, storage requirements and the data migration plan;

(e) for each application that has a Disaster Recovery Plan, develop the plan to identify and implement changes to the Service Provider's portion of such Disaster Recovery Plan;

(f) provide a checklist of typical changes required to support the migration referred to in Section 15.3.2.2(e) (*Province Responsibilities*); and

(g) create, as part of the Wave Plan, the detailed engineering plan based on the mapping from the source Server to the target physical or virtual Server and taking account of source Server capacity and functionality, application interdependencies, business criticality and performance requirements.

15.3.2.2 Province Responsibilities

The Province will:

(a) for each Application to be migrated to a physical or virtual Server, identify acceptable change windows during which the migration can take place;

(b) facilitate the participation of the Clients in the development of the proposed task schedule;

(c) define the process and contacts for escalating issues arising from the Wave;

(d) for each application that has a Disaster Recovery Plan, develop the plan to identify and implement changes to the Province's portion of such Disaster Recovery Plan;

(e) develop the plan to identify and implement changes to Applications or desktops required to support the migration of Servers (Applications and associated data); and

(f) approve the Wave Plan.

15.3.3 Hardware and Software

The Service Provider will, with input from the Province (including Clients), procure, install and configure hardware and software identified in the Wave Plan in accordance with their responsibilities as described in the Server Management Services SOW and the Managed Storage and Managed Backup SOW.

15.3.4 Virtualization and Migration Testing

The Province and the Service Provider will test the migration of each application and its associated data to a physical or virtual Server as specified in the Committed Annual Plan.

15.3.4.1 Service Provider Responsibilities

The Service Provider will:

(a) work with the Province to define test cases and acceptance test criteria to verify the virtualization and migration process including application user verification to be performed by Clients;

(b) provide the Client application support teams with an environment to run their application system and data migration tests; and

(c) conduct the virtualization and migration tests with the Client so as to meet the agreed acceptance test criteria.

15.3.4.2 Province Responsibilities

The Province will:

(a) facilitate the Clients' application support teams' participation in the application system and data migration test;

(b) facilitate the Clients' participation in the virtualization and migration tests;

(c) implement and test any changes required, as a result of a migration, to Clients' Applications or related environmental changes to other Client assets; and

(d) coordinate the Client's participation in the virtualization and migration testing.

15.3.5 Virtualization and Migration Pilot

The Province and the Service Provider will perform a pilot migration of each application and its associated data to a physical or virtual Server as specified in the Committed Annual Plan including:

(a) a migration of each current application;

(b) a migration of all required data, for each application;

(c) a test of the fallback contingency plans; and

(d) for Applications that have a defined Disaster Recovery Plan, a test of the modified Disaster Recovery Plan (provided that, for minor modifications to the Disaster Recovery Plan, the Province and the Service Provider may agree to defer testing the Disaster Recovery Plan until its regular cycle).

If the virtualization and migration pilot identifies a need for changes to Clients' Applications or related environmental changes to other Clients' assets, the Province will facilitate the Clients' completion of the required changes following which the Province and the Service Provider will repeat the virtualization and migration pilot testing or withdraw the application and its associated data from the migration Wave. The Parties will replan the Virtualization and Migration of Applications and their associated data that withdraw from a migration Wave as contemplated in the Committed Annual Planning process that is described in Section 15.1 (*Committed Annual Plans*).

15.3.5.2 Service Provider Responsibilities

The Service Provider will:

(a) work with the Clients to define test cases and acceptance test criteria to verify the virtualization and migration process, the operation of the fallback contingency plan and the operation of the Disaster Recovery Plan, if any, including verification of tests by Clients;

(b) provide the Clients' application support team and Clients with an environment to run the virtualization and migration pilot test; and

(c) conduct the virtualization and migration pilot test with the Province (repeating, if necessary) so as to meet the agreed acceptance test criteria.

15.3.5.3 Province Responsibilities

The Province will:

(a) facilitate the Clients' application support teams' participation in the application system and data migration pilot;

(b) facilitate the Clients' participation in the virtualization and migration pilot;

(c) implement and test any changes required, as a result of the migration of an application and associated data, to Clients' Applications or related environmental changes to other Client assets; and

(d) coordinate the Client's participation in the virtualization and migration pilot.

15.3.6 Migration with Fallback Contingency

The Province and the Service Provider will complete the application and data Migrations to a Physical Servers or Virtual Server as specified in the Committed Annual Plan in accordance with the Wave Plan. In the event of a virtualization and migration failure detected by either Party, the Parties in consultation with each other, will execute the fallback contingency plan.

Upon successful Migration of the Applications and associated data, for Applications that have a defined Disaster Recovery Plan the Province and the Service Provider will activate the modified Disaster Recovery Plan to take account of the Migration of such applications.

15.3.7 Decommission of Equipment

After each Wave is successfully completed, the Service Provider will decommission any Province equipment that is managed by the Service Provider and that the Service Provider no longer requires for the performance of the Managed Services in accordance with the Services Management SOW or Server Management Services SOW, as applicable.

15.3.8 Completion

For the purposes of this SOW, each Virtualization and Migration Wave will be deemed to be "complete" when the activities detailed in Section 15.3 (*Plan of a Typical Virtualization and Migration Wave*) have been completed by the Parties for each Application contemplated to be Migrated to Physical Servers or Virtual Servers in the Committed Wave excluding any that are withdrawn by the Province and not substituted by the Service Provider after the Wave is confirmed by the Province as a Committed Wave.

15.4 Mainframe Migration Wave

The Parties contemplate a separate migration Wave coinciding with the planned Mainframe Services Migration, as reflected in the Multi-Year Plan. This separate migration Wave will include only those Servers (Applications) that should be co-located with the Mainframe System to maintain the performance of the Servers (Applications) operating on the Mainframe System

and co-located Servers. These Servers (Applications and their associated data) will be identified by the Service Provider and the Province in the Virtualization Assessment and Migration Planning Project described in Section 10 (*Virtualization Assessment and Migration Planning Project*) of this SOW and the Server Management Services SOW and the Managed Storage and Managed Backup SOW.

The Mainframe Migration Wave will utilize the process described above for a Typical Virtualization and Migration Wave in Section 15.3 (*Plan of a Typical Virtualization and Migration Wave*).

15.4.1 Completion

For the purposes of this SOW, each Mainframe Migration Wave will be deemed to be "complete" when the activities detailed in Section 15.3 (*Plan of a Typical Virtualization and Migration Wave*) have been completed by the Parties for each Application contemplated to be Migrated to Physical Servers or Virtual Servers in the Committed Wave excluding any that are withdrawn by the Province and not substituted by the Service Provider after the Wave is confirmed by the Province as a Committed Wave.

15.5 "Migration Only" Waves

The Parties contemplate separate "migration only" Waves for Servers (Applications) that have been transformed "in place" at the Province Data Centres, as reflected in the Multi-Year Plan. These Servers (Applications) will be identified by the Service Provider and the Province in the Virtualization Assessment and Migration Planning Project. These "migration only" Waves will utilize the process described above for a Typical Virtualization and Migration Wave in Section 15.3 (*Plan of a Typical Virtualization and Migration Wave*) except that:

(a) Virtual Servers at the Province Data Centres will be migrated to another Virtual Server target environment at an STMS Data Centre;

(b) Physical Servers at the Province Data Centres will be migrated to similar Physical Servers at an STMS Data Centre; and

(c) after migration, the Service Provider will move any of the Service Provider Servers displaced as a result of the "migration only" Waves from the Province Data Centres to the STMS Data Centres in preparation for subsequent migrations.

15.5.2 Completion

For the purposes of this SOW, each "migration only" Wave will be deemed to be "complete" when the activities detailed in Section 15.5 (*"Migration Only" Waves*) have been completed by the Parties for each Application contemplated to be Migrated to Physical Server or Virtual Servers in the Committed Wave excluding any that are withdrawn by the Province and not substituted by the Service Provider after the Wave is confirmed by the Province as a Committed Wave.

15.6 Migrate "Unrefreshable" Servers

Certain Applications are not susceptible to migration as described above because they have dependencies on existing Server hardware or operating systems. For example, an application that depends on Windows NT, which is no longer supported, and cannot operate on a supported version of Windows, will not be susceptible to migration using the process as described above.

The Servers on which such Servers (Applications) are operating are referred to as the "Unrefreshable" Servers.

If the Province requires the Service Provider to manage any "Unrefreshable" Servers after the end of the five year virtualization and migration period, the Province and the Service Provider will collaborate to develop a custom migration plan to physically transport the "Unrefreshable" Servers to one of the STMS Data Centres along with their data and the Servers (Applications) they host. The custom migration plan will contemplate that the transportation of the "Unrefreshable" Servers will be completed prior to the end of the five year virtualization and migration period.

15.6.1 Completion

For the purposes of this SOW, the Migrate "Unrefreshable" Servers Wave will be deemed to be "complete" when the activities detailed in Section 15.6 (*Migrate "Unrefreshable" Servers*) have been completed by the Parties for each Application contemplated to be Migrated to Physical Servers or Virtual Servers in the Committed Wave excluding any that are withdrawn by the Province and not substituted by the Service Provider after the Wave is confirmed by the Province as a Committed Wave.

16. TRANSFORMATION MANAGEMENT AND GOVERNANCE

The Transformation Projects defined in this Transformation Program are subject to the Transformation Program Governance Process described in this Section 16 (*Transformation Management and Governance*). It is also the intent of the Parties that future Transformation Projects may be proposed and considered by the Parties through the Governance Process set out in the Agreement and, if approved, they will also be subject to the Transformation Program Governance Process described in Section 16. Within sixty days following the Hand-Over Date, the Province and the Service Provider will review the Transformation Program Governance Process that is documented in this Article and confirm their agreement to the process, including its application to the specific Transformation Projects, either as currently documented or with such change as may be agreed to by the Parties in writing.

The Service Provider has appointed a Transformation Project Manager who is responsible for Service Provider reporting, escalation processes and is the liaison to the Province for all Transformation activities.

The Province has appointed a Transformation Project Manager who is responsible for Province reporting, escalation processes and is the liaison to the Service Provider for all Transformation activities.

The Service Provider Transformation Project manager will, in consultation with the Province, develop and manage a detailed plan that addresses Service Provider and Province roles and responsibilities.

16.1 Transformation Program Governance

All Transformation Projects are subject to the Transformation Program Governance Process described in this section.

16.1.1 Introduction

The intent of the Transformation Program Governance Process is to ensure the Transformation Projects follow a prescribed project management methodology and are managed consistently and rigorously to achieve business results in the most efficient manner.

The project management methodology allows the Transformation Working Group to oversee project progress and maintain a record of findings, decisions and recommendations.

16.1.2 Transformation Working Group

The Service Provider and Province Transformation Project Managers will co-lead a "Joint Working Group" (to be known as the "**Transformation Working Group**") as defined in Section 2.1 of Schedule 18 (*Governance*) of the Agreement. The Transformation Working Group, with the support of the Service Provider Program Management Office, will hold regular reviews to monitor the progress of the Transformation Projects and to identify issues that may affect the schedule for completion of the Transformation Project activities. The Transformation Working Group will resolve any potential delays or circumstances that may adversely affect Transformation Projects or they will escalate any unresolved issues in accordance with the Governance Process.

The mandate of the Transformation Working Group is to ensure that project definition and execution are appropriately managed through oversight and defined approval events ("**Project Gates**") throughout the project life cycle.

The five Project Gates summarized in the following chart are the "Decision Gates" that the Transformation Working Group will use to oversee the proper definition and execution of each Transformation Project.

Initiation	Planning	Design	Go Live Assessment	Close Down
Key deliverables reviewed and approved Project manager assigned Province OK to	An integrated Project Plan is approved Resources are secured and roles and responsibilities	Approval of Design Approval of PIA / TRA/ FRCA Project performance and	Testing is thorough and materially complete IT and business is ready for	Closure Documents reviewed Acceptance of outstanding issues/ recommendations

Initiation	Planning	Design	Go Live Assessment	Close Down
start the project Approval to proceed as a Project Project Dashboard status change from "Approved" to "Active"	are assigned Approval to baseline project plans and to proceed to Design phase	health assessed and areas for improvement addressed	deployment Approval to Go Live	and assignment for action and logging for follow up Project considered complete Project Dashboard status change from "Active" to "Closed"

16.1.3 Membership and Roles

The Transformation Working Group is comprised of representatives from both the Province and Service Provider. The Transformation Working Group roles consist of Transformation Working Group co-chairs, administrator and members.

Role	Program Area	Organization
Co-Chair		
Transformation Working Group Co-Chair	Transformation Project manager	Province
Transformation Working Group Co-Chair	Transformation Project manager	Service Provider
Administration		
Transformation Administrator	Program Management Office ("**PMO**")	Service Provider
Members		
PMO Leader	Service Provider PMO	Service Provider
A&E representation	Architecture and Engineering ("**A&E**")	Technology Architecture Working Group
PSCO representation	Office of Privacy and Security ("**PSCO**")	Service Provider Province
PM Subject Matter Experts	Service Provider PMO	Service Provider

16.1.4 Transformation Working Group Responsibilities

The Transformation Working Group reviews and validates the quality of key project deliverables and provides direction to the Transformation Project managers regarding improvements, clarifications or additional documentation requirements.

The overall responsibilities of the Transformation Working Group include:

(a) reviewing key project deliverables;

(b) confirming project definitions;

(c) confirming that projects are planned at an appropriate level of detail;

(d) confirming projects are adequately controlled, reporting meaningful status and addressing forecast performance issues or emergent problems;

(e) promoting continuous project management improvement by utilizing a lessons learned process;

(f) resolving escalated issues and problems;

(g) reviewing project status reports;

(h) identifying risks and developing mitigations; and

(i) escalating issues and problems that cannot be resolved by the Transformation Working Group.

16.1.5 Member Responsibilities

Sections 16.1.5.1 to 16.1.5.6 below outline responsibilities related to the specific roles within the Transformation Working Group.

16.1.5.1 Co-Chair

The Co-Chair's responsibilities will include the following:

(a) lead the Transformation Working Group in fulfilling its mandate;

(b) maintain Transformation Working Group priorities;

(c) bring forth and provide information as required;

(d) identify project issues that require discussion and/or resolution by the Transformation Working Group;

(e) review, approve and authorize project initiation, planning, design, go-live and closure deliverables; and

(f) review and authorize project Change Requests to proceed through the Change Order Process.

16.1.5.2 Transformation Administrator

The Transformation Administrator's responsibilities will include the following:

(a) prepare agenda in consultation with the Co-Chairs;

(b) schedule meetings and coordinate Transformation Working Group guest attendees;

(c) create and distribute meeting agenda, project deliverables and supporting materials for review at least two business days prior to the meeting; and

(d) document and distribute meeting minutes and action items within two business days;

16.1.5.3 Members

A Member's responsibilities will include the following:

(a) bring the viewpoints of the business function they represent to the table as well as keep their stakeholders informed of Transformation Working Group recommendations and developments; and

(b) send an alternate or provide their written input to a co-Chair prior to the meeting if they are unable to attend a meeting.

16.1.5.4 Guest Members

Guest members include project managers and project sponsors who will be invited when their projects are on the agenda. The Transformation Working Group may extend invitations to other stakeholders to attend meetings where their input would be of benefit.

16.1.5.5 Project Manager

The Project Manager's responsibilities will include the following:

(a) complete project initiation, planning, design, go-live and close down deliverables on a timely basis;

(b) complete Change Requests (CRs) as required;

(c) compile bi-weekly status reports representing the status of their projects; and

(d) attend meetings and provide additional information as required.

16.1.5.6 Project Sponsors (assigned from the Province AMO)

The Project Sponsors' responsibilities will include the following:

(a) review, approval and authorization (signature) of project initiation, planning, design, go-live and closure deliverables;

(b) authorize project Change Requests pending AMO Change Order approval if required; and

(c) attend meetings as required.

16.2 Working Group Meetings

The working group is required to meet bi-weekly. Meeting frequency will be increased to accommodate Program requirements, if needed.

16.3 Acceptance Testing

Where required by the Parties, acceptance test requirements have been defined in each Transformation Project.

16.4 Project Decision Gates

The following chart illustrates the five project Decision Gates, their associated project management deliverables and acceptance criteria to be applied by the Transformation Working Group.

	Initiation	Planning	Design	Go Live Assessment	Close Down
Purpose	Ensure that the project aligns with business strategy, defines a clear scope statement and ensures the appropriate sponsorship and resource levels. Initiation Documents Review /Approval	Establish what the project will and will not do, resource requirements and how and when work will be completed. Planning Documents Review/ Approval Technical Architecture in place	Accept changes to the process design, supporting IT design and implementation strategy. Design Documents Review/Approval Privacy and Security Assessments Review/Approval	Verify IT and Business Readiness, and confirm that the solution is meeting the defined acceptance criteria. Provide insight into project execution and readiness for implementation Ensure engineered solution follows approved architecture, standards, privacy and security	Confirm the level of performance achieved, confirm that the initiative has completed its work, and endorse an action plan for ongoing management or the creation of a new initiative. Provide insight into project successes and opportunities Officially close down project

	Initiation	Planning	Design	Go Live Assessment	Close Down
				expectations	
Required Key Deliverables	PM Deliverables Project Initiation Document (PID) including project objectives, affected business /areas, roles and responsibilities Project High Level Risk Assessment including initial privacy impact assessment Project Solution Deliverables Service Request or equivalent including funding, high level objectives and timing	PM Deliverables Project Plan containing: - Scope Statement and Requirements - Communication Plan - Roles and Responsibilities - Staffing Plan - Cost Management Plan - Quality Plan - Assumptions and Constraints Issues/Decisions Log Project Schedule Risk Management Plan Change Management Plan (optional) Test Strategy Project Solution Deliverables Technical Architecture Document Initial Privacy and Security Assessments (high level)	PM Deliverables Test Plan Implementation Plan Detailed Requirements PM Healthcheck Report Change Request (if required) Project Solution Deliverables Technical Design Specifications Functional Design Specifications Technical Architecture Document Detailed Privacy Assessment Detailed Security Threat Risk Assessment (including full controls review); outputs of this assessment are a completed TRA document and any required deviation tracking. Financial Risk & Controls Review (where applicable)	PM Deliverables UAT Test Results Project Solution Deliverables Final Solution Delivery Validation Assessment (documenting discrepancies between implemented solution and Approved Design, including all required mitigation\follow-up activities)	PM Deliverables Project Completion Statement (including feedback from Lessons Learned Report) Ensure any remaining items from the Final Solution Delivery Assessment are assigned appropriately Project Solution Deliverables Final Technical Architecture Document Final Technical Design Specifications Final Functional Design Specifications Operational Documentation (as required) – for example, system administration documents and "run books" in the Service Provider.
Acceptance Criteria	**Key deliverables and Project Decision Gate Criteria reviewed and approved**	**An integrated Project Plan is approved** **Resources are secured and roles and**	**Approval of Design** **Approval of PIA / TRA/ FRCA** **Project performance and**	**Testing is thorough and materially complete** **IT and business is ready for**	**Closure Documents reviewed** **Acceptance of outstanding issues/**

	Initiation	Planning	Design	Go Live Assessment	Close Down
	Project funding allocated **Project manager assigned** **Province OK to start the project** **Approval to proceed as a Project** **Project Dashboard status change from "Approved" to "Active"**	**responsibilities are assigned** **Approval to baseline project plans and to proceed to Design phase**	**health evaluated and areas for improvement addressed**	**deployment** **Approval to go "live"**	**recommendations and assignment for action and logging for follow up** **Project considered complete** **Project Dashboard status change from "Active" to "Closed"**

During the formal review of the Project Initiation Decision Gate deliverables, the Transformation Working Group will confirm all project deliverables and the Decision Gate criteria that will apply to each project. This will permit tailoring of project deliverables as appropriate to the scope of the project. For example, if a Security Threat and Risk Assessment is required during the execution of the project, that will be confirmed during the Initiation Decision Gate.

16.5 Completion

For the purposes of this SOW, the Last Weekly Status Report of the Month Milestone (see table above), as described in Schedule 23 (*Fees*), Appendix I, will be deemed to be "complete" when the Service Provider submits to the Province the last bi-weekly status report for each and every month from month one through sixty of the term of the Agreement.

Appendix A — Definitions

Definable Term	Definition
Agreement	Has the meaning attached thereto in the introductory paragraph of this SOW.
Asset Centre	Has the meaning attached thereto in Section 7.2.5 of this SOW.
Bridge Plan	Has the meaning attached thereto in Section 8.1 of this SOW.
Business Office	Has the meaning attached thereto in Section 3.2 of this SOW.
Change Management Process	Has the meaning set out in the Service Management SOW.
Change Order Process	Has the meaning set out in the Agreement.
Customer Environment for Managed Services	Means the Customer Environment to be constructed by the Service Provider under the Data Centre Services SOW for the provision of Managed Services at the STMS Data Centres
Committed Annual Plan	Has the meaning attached thereto in Section 15.1.
Current MF Provider	The service provider performing the mainframe services immediately prior to the commencement of the Managed Mainframe Services as described in the Managed Mainframe Services SOW.
Customer Environment	Has the meaning attached to such term in the Data Centre Services SOW.
Data Centre Services	Has the meaning attached thereto in the Agreement.
Data Centre Services Subcontractor	Q9 Networks Inc.
Decision Gates	Has the meaning attached thereto in Section 16.4.
Detailed Transformation Plan	Means Schedules 9 and 10 of the Agreement as of the Hand-Over Date.
Disaster Recovery Plan	Has the meaning attached thereto in the Agreement.
Disaster Recovery Site	Has the meaning attached thereto in the Business Continuity and Disaster Recovery SOW.

Definable Term	Definition
Dispatch Interface	Has the meaning attached thereto in Section 7.2.2 of this SOW.
DR Tapes	Has the meaning attached thereto in Section 8.1 of this SOW.
Fallback Plan	Has the meaning attached thereto in Section 8.2 of this SOW.
Field Services	Has the meaning attached thereto in Section 11 of this SOW.
Governance Process	Has the meaning attached thereto in the Agreement.
Hand-Over Date	Has the meaning attached thereto in the Agreement.
Hosting Locations	Means at any time, the Province Data Centres, STMS Data Centres, the Remote Infrastructure Server Locations and Remote Application Server Locations at which the Managed Equipment is located at such time.
Incident	Has the meaning attached thereto in the Service Management SOW.
Local Area Network (LAN)	Has the meaning attached thereto in the Managed Storage and Managed Backup SOW.
Mainframe System	Has the meaning attached thereto in the Managed Mainframe Services SOW.
Mainframe System Software	Has the meaning attached thereto in the Managed Mainframe Services SOW.
Managed Equipment	Has the meaning attached thereto in the Data Centre Services SOW.
Managed Mainframe Services	Has the meaning attached thereto in the Managed Mainframe Services SOW.
Mainframe Services Migration	Has the meaning attached thereto in Section 8.1 of this SOW.
Mainframe Services Migration Plan	Has the meaning attached thereto in Section 8.2 of this SOW.
Managed Services	Has the meaning attached thereto in the Agreement.

Definable Term	Definition
Management Network	Has the meaning attached thereto in Section 6.2 of this SOW.
Manual	Has the meaning attached thereto in the Agreement.
Mock 0 Test	Has the meaning attached thereto in Section 8.1 of this SOW.
Mock 1 Test	Has the meaning attached thereto in Section 8.1 of this SOW.
Multi-Year Plan	Has the meaning set out in Section 10 of this SOW.
Non-Dispatch Interface	Has the meaning attached thereto in Section 7.2.3 of this SOW.
Non-DR Tapes	Has the meaning attached thereto in Section 8.1 of this SOW.
Other Customers	Entities, other than the Province, buying only Data Centre Services from the Service Provider.
PCM Tools	Has the meaning attached thereto in Section 9.2.7 of this SOW.
Privileged ID	Has the meaning attached thereto in the Security SOW.
Program Management Office	Has the meaning attached thereto in Section 0 of this SOW.
Province Data Centres	Has the meaning attached thereto in the Data Centre Services SOW.
Province's CSC	Has the meaning attached thereto in the Service Management SOW.
Province Designated Network Locations	The Province Data Centres S. 15 S. 15
Province Network	SPAN-BC.
Province Ordering System	Has the meaning attached thereto in the Service Management SOW.
Province Service Desk Tool	Has the meaning attached thereto in the Service Management SOW.
Province Service	Has the meaning attached thereto in the Service Management

Definable Term	Definition
Management Systems	SOW.
Province Staff	Has the meaning attached thereto in Service Management SOW.
Reference Architecture	Has the meaning attached thereto in Section 10.4 of this SOW.
Province Servers	Means, at any time, the Servers owned by the Province and for which the Service Provider is providing Managed Services at such time.
Reference Architecture	Has the meaning attached thereto in Section 10.4.
Remote Infrastructure Server Locations and Remote Application Server Locations	As described in Schedule 8 (*Service Locations*).
Back-up Migration Plan	A plan to reverse the progress of At issue for Inquiry
Revised Transformation Plan	Has the meaning attached thereto in Section 3.4 of this SOW.
Server Monitoring Tools	As described in the Server Management Services SOW.
Server Systems Management	Has the meaning attached thereto in Section 9 of this SOW.
Servers	Has the meaning attached thereto in the Server Management Services SOW.
Service Provider Service Desk Tool	Has the meaning attached thereto in the Service Management SOW.
Service Provider Network Equipment	Means the routers to be installed at the Province Designated Network Locations as the terminating network appliances for the Management Network.
Service Provider Office Facilities	The facilities a At issue for Inquiry Victoria, British Columbia that are being leased by the Service Provider in order to provide the Services to the Province under the Agreement.

Definable Term	Definition
Service Provider Support Locations	Has the meaning attached thereto in the Data Centre Services SOW.
Services	Has the meaning attached thereto in the Agreement.
Software Agents	Has the meaning attached thereto in the Server Systems Management SOW.
Software and Patch Distribution Tools	Has the meaning attached thereto in the Server Systems Management SOW.
Source to Target Report	Has the meaning attached thereto in Section 10.4.1 of this SOW.
STMS Calgary Data Centre	Means the STMS Data Centre located in Calgary, Alberta.
STMS Data Centre Availability Date	Has the meaning attached to such term in Schedule 23 (*Fees)* of the Agreement.
STMS Data Centres	Means the STMS Calgary Data Centre and the STMS Interior Data Centre.
STMS Interior Data Centre	Means the STMS Data Centre located in the interior of British Columbia.
Third Party Gateway	The security mechanisms that the Province implements to control third party access to SPAN BC.
Transformation Plan	Has the meaning set out in Section 3.4 of this SOW.

Definable Term	Definition
Transformation Program	Refers collectively to all the Transformation Project set out in this SOW.
Transformation Projects	The projects described in Sections 4 through 16 of this SOW as "Transformation Projects".
Transitioning Employees	Means the employees of the Province who are transitioning to the Service Provider on the Hand-Over Date.
Virtualization	Has the meaning attached thereto in Section 10.
Virtualization and Migration Assessment Plan	Has the meaning attached thereto in Section 10.
Virtualized	Has the meaning attached thereto in Section 10.
Wave Plan	Has the meaning attached thereto in Section 15.3.2 of this SOW.
Waves	Cycles of Server migration described in the Plan.
Work-in-Progress Projects	Has the meaning attached thereto in Schedule 1 of the Agreement.
WTS Data Centres Equipment	Has the meaning attached thereto in the Data Centre Services SOW.
WTS Office Facilities	Has the meaning attached thereto in Section 4.1 of this SOW.

Appendix B

Intentionally Deleted

Appendix C - Manual Outline

Please see attached.

OPERATIONAL PROCEDURES MANUAL

Table of Contents

8.11 Database Monitoring (Uplift)

8.11.1 Description

8.11.2 How User Requests Services

8.11.3 Processes and Procedures

8.12 Database Management (Uplift)

8.12.1 Description

8.12.2 How User Requests Services

8.12.3 Processes and Procedures

8.13 Database Performance Management (Uplift)

8.13.1 Description

8.13.2 How User Requests Services

8.13.3 Processes and Procedures

8.14 Configuration Information

9. STORAGE SERVICES

9.1 Managed Storage Services

9.1.1 Description

Managed Storage Services is the management of the storage of Data in storage tiers (Tier 1, 2, 3) based upon performance and reliability required for such Data. The storage tiers are distinguished by the performance of the disk and the Storage Array (the amount of cache memory, speed and size of the disk and the size of the RAID group) and the reliability of the disk and the Storage Array (the type of Storage Array with its underlying redundancy components and the size of the RAID group). The Managed Storage Services establish the data storage foundation required to support the Province Data storage requirements. The Service Provider will use integrated Storage Hardware, Storage Software, and support solutions to provide the Managed Storage Services within the range of data storage tiers identified, as appropriate.

9.1.2 Managed Storage Tier 1 Services

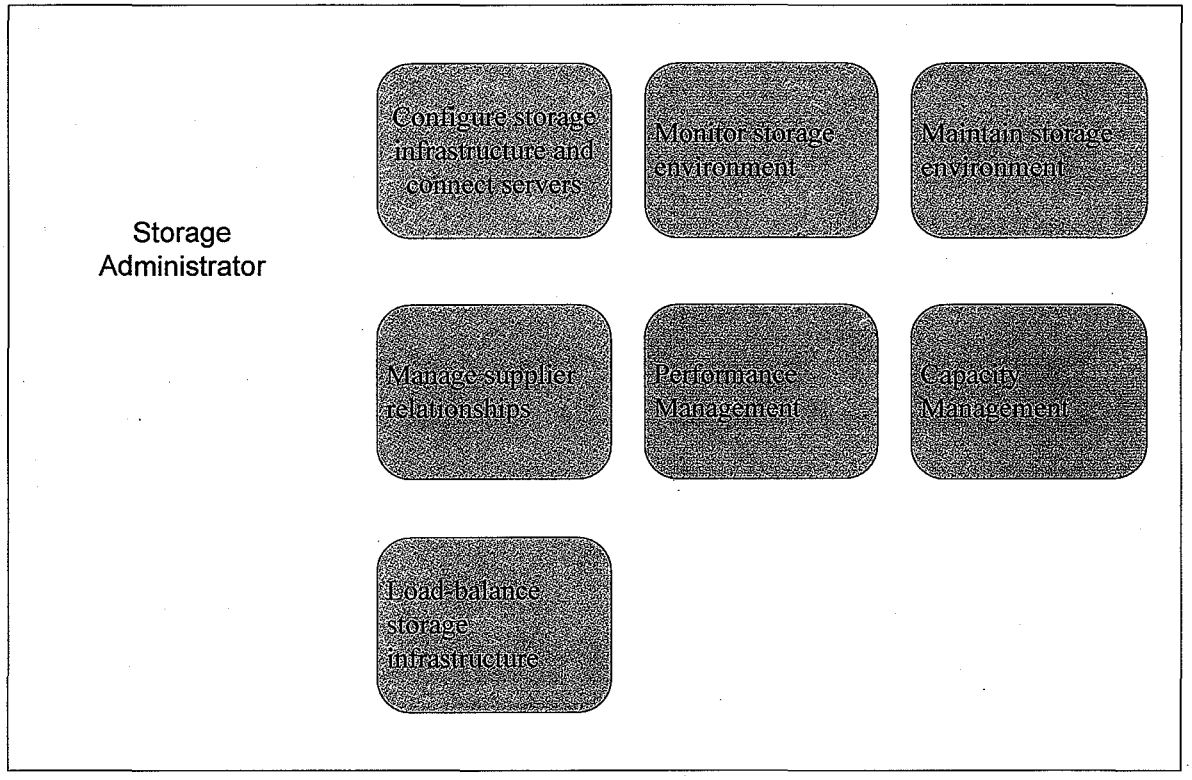
9.1.2.1 Description

Managed Storage Tier 1 Service is a class of disk storage that is the highest performing, highest availability and is designed with the most redundancy. The Managed Storage Tier 1 Service has additional redundancy through the incorporation of storage multipathing using Storage Multi-Path Resilience. Service Provider provides monitoring, configuration, control, and tuning software with continuous operational support for the Managed Storage Tier 1 Service.

9.1.2.2 How User Requests Services

Type of Request	Method
Minor service requests for Managed Storage Tier 1 Service	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Managed Storage Tier 1 Service	Province's iStore system (managed storage requirements definition request)
Adhoc requests	Emails from authorized users to group mailbox

9.1.2.3 Processes and Procedures



9.1.2.3.1. Configure storage infrastructure and connect servers

Step 1
Step 2
Step 3 etc.

9.1.2.3.2. Monitor storage environment

Step 1
Step 2
Step 3 etc.

9.1.2.3.3. Maintain storage environment

Step 1
Step 2
Step 3 etc.

9.1.2.3.4. Manage supplier relationships.

Step 1
Step 2
Step 3 etc.

9.1.2.3.5. Performance management

Step 1
Step 2
Step 3 etc.

9.1.2.3.6. Capacity management

Step 1
Step 2
Step 3 etc.

9.1.2.3.7. Load balance storage infrastructure

Step 1
Step 2
Step 3 etc.

9.1.3 Managed Storage Tier 1 Services with Replication Services (Optional Service)

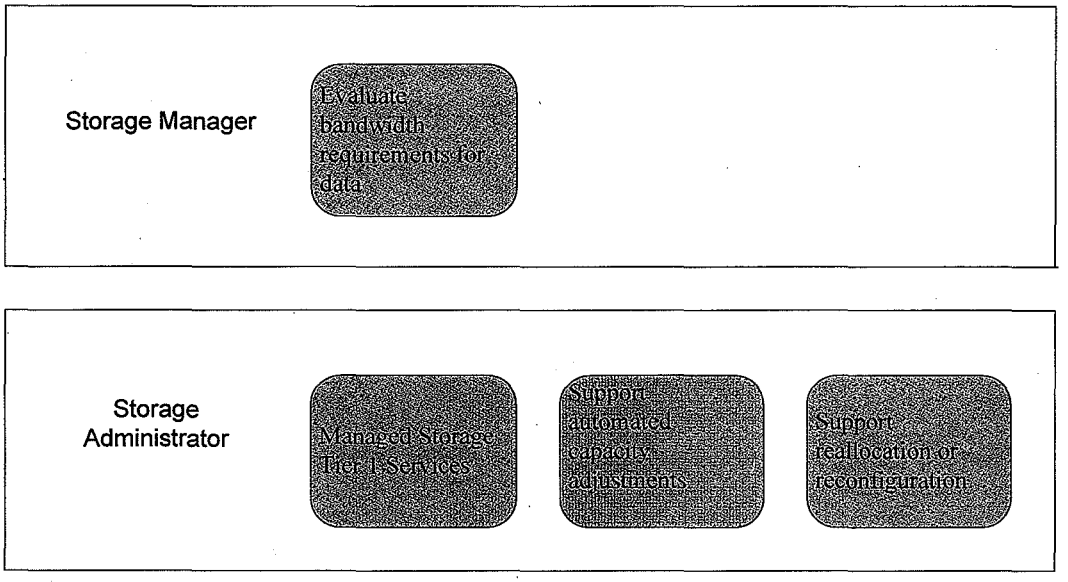
9.1.3.1 Description

Under the Managed Storage Tier 1 Services with Replication Services the Service Provider will move and replicate the Province Data to a Managed Storage Tier 1 Services at a Service Provider Data Centre. The Service Provider will Replicate the Province Data using the Storage Array based technology which includes Storage Array specific Storage Hardware and Storage Software which synchronizes the primary copy of the Province Data with the secondary copy of the Province Data using SRDF (or other storage replication) technology (for clarity, Managed Storage Tier 1 Services with Replication Services is not Application based replication). The software managing the Replication is on the Storage Array not on an application or other source. If the primary copy of the Province Data is the Calgary Data Centre then the secondary copy of the Province Data will be Replicated to the Interior Data Centre and if the primary copy of the Province Data is the Interior Data Centre then the secondary copy of the Province Data will be Replicated to the Calgary Data Centre. Managed Storage Tier 1 Services with Replication Services lowers the time to restore operations as it relates to making data available to a Host at the secondary Service Provider Data Centre. Managed Storage Tier 1 Services with Replication Services provides for the creation of and enablement of data content replication and Service Provider Data Centre site replication.

9.1.3.2 How User Requests Services

Type of Request	Method
Minor service requests for Replication Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Replication Services	Province's iStore system (managed storage requirements definition request)

9.1.3.3 Processes and Procedures



9.1.3.3.1. Evaluate bandwidth requirements for data

Step 1
Step 2
Step 3 etc.

9.1.3.3.2. Managed Storage Tier 1 services

Step 1
Step 2
Step 3 etc.

9.1.3.3.3. Support automated capacity adjustments

Step 1
Step 2
Step 3 etc.

9.1.3.3.4. Support relocation or reconfiguration

Step 1
Step 2
Step 3 etc.

9.1.4 Managed Storage Tier 1 Services with Local Clone Services (Optional Service)

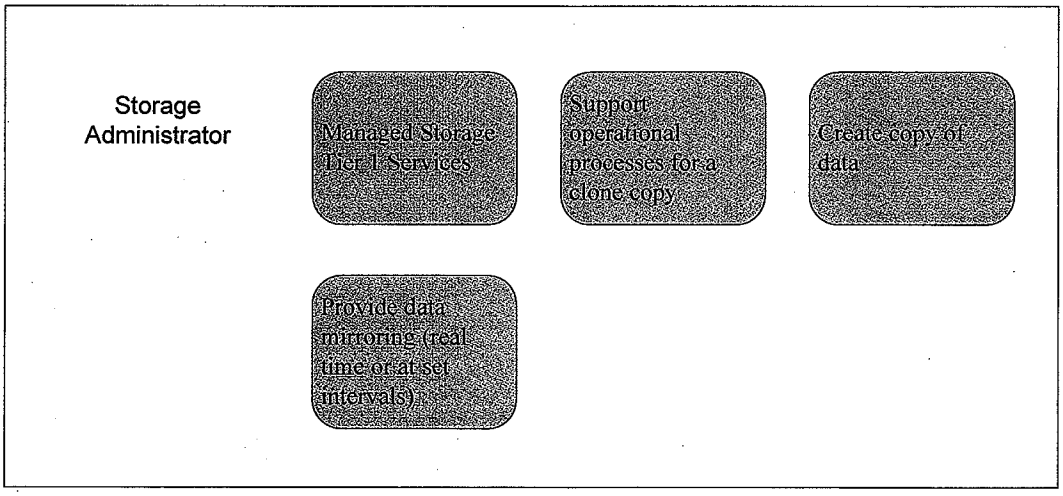
9.1.4.1 Description

Under Managed Storage Tier 1 Services with Local Clone Services the Service Provider will Mirror a copy of the Province Data in the same Storage Array at the Service Provider Data Centre where the primary SAN storage disk resides. Managed Storage Tier 1 Services with Local Clone Services provides a copy of Province Data that can be managed by the primary Host or the management of the copy may be assigned to a second Host for Backup or testing purposes.

9.1.4.2 How User Requests Services

Type of Request	Method
Minor service requests for Local Clone Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Local Clone Services	Province's iStore system (managed storage requirements definition request)

9.1.4.3 Processes and Procedures



9.1.4.3.1. Managed Storage Tier 1 services

Step 1
Step 2
Step 3 etc.

9.1.4.3.2. Support operational processes for a clone copy

Step 1
Step 2
Step 3 etc.

9.1.4.3.3. Create copy of data

Step 1
Step 2
Step 3 etc.

9.1.4.3.4. Provide mirroring (real time or set intervals)

Step 1
Step 2
Step 3 etc.

9.1.5 Managed Storage Tier 2 and Tier 3 Services

9.1.5.1 Description

Service Provider Tier 2 and Tier 3 Managed Storage Services provides the Province with a leveraged, SAN based, storage platform.

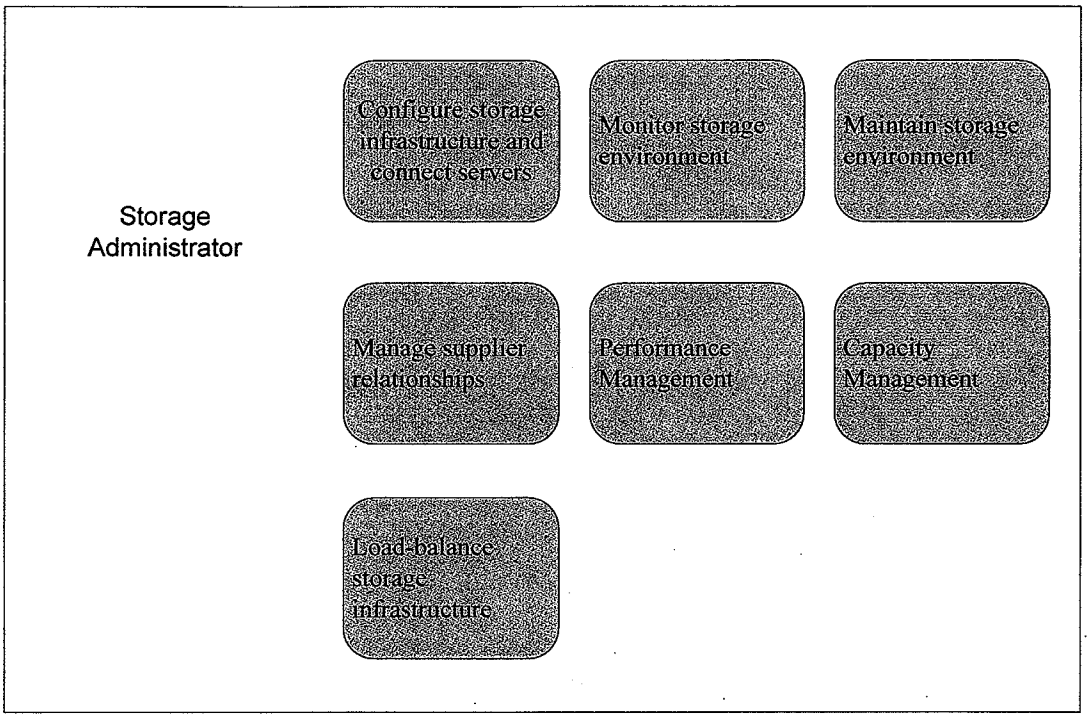
Managed Storage Tier 2 Services is a class of disk storage that has medium performance, high availability and is designed with a high level of redundancy. The Managed Storage Tier 2 Service has additional redundancy through the incorporation of storage multipathing through the use of Storage Multi-Path Resilience. Service Provider provides monitoring, configuration, control, and tuning software with continuous operational support for the Managed Storage Tier 2 Service.

Managed Storage Tier 3 Services is a class of disk storage that has an economy performing disk, lower availability than Tier 2 Service and is designed with a high level of redundancy. The Managed Storage Tier 3 Service has additional redundancy through the incorporation of storage multipathing through the use of Storage Multi-Path Resilience. Service Provider provides monitoring, configuration, control, and tuning software with continuous operational support for the Managed Storage Tier 3 Service.

9.1.5.2 How User Requests Services

Type of Request	Method
Minor service requests for Managed Storage Tier 2 and Tier 3 Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Managed Storage Tier 2 and Tier 3 Services	Province's iStore system (managed storage requirements definition request)

9.1.5.3 Processes and Procedures



9.1.5.3.1. Configure storage infrastructure and connect servers

Step 1
Step 2
Step 3 etc.

9.1.5.3.2. Monitor storage environment

Step 1
Step 2
Step 3 etc.

9.1.5.3.3. Maintain storage environment

Step 1
Step 2
Step 3 etc.

9.1.5.3.4. Manage supplier relationships

Step 1
Step 2
Step 3 etc.

9.1.5.3.5. Performance management

Step 1
Step 2
Step 3 etc.

9.1.5.3.6. Capacity management

Step 1

Step 2
Step 3 etc.

9.1.5.3.7. Load balance storage infrastructure

Step 1
Step 2
Step 3 etc.

9.1.6 Storage Multi-Path Resilience Services

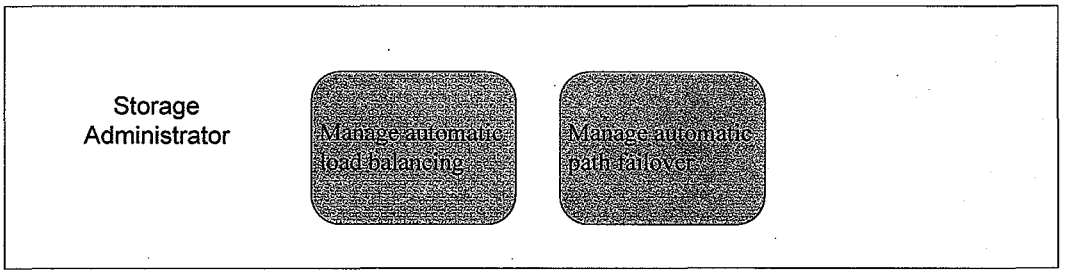
9.1.6.1 Description

Storage Multi-Path Resilience Services is the provisioning of additional performance and information availability enhancements for the Province's servers by providing redundant paths for a Host to access storage data so that it would take a multiple connectivity component failure to render a server inaccessible to its associated storage. Designed for open server platforms connected to Service Provider SAN storage systems, Multi-Path Resilience provides intelligent multi-path load balancing which ensures channels are utilized in the most efficient manner possible

9.1.6.2 How User Requests Services

Type of Request	Method
Minor service requests for Storage Multi-Path Resilience Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Storage Multi-Path Resilience Services	Province's iStore system (managed storage requirements definition request)

9.1.6.3 Processes and Procedures



9.1.6.3.1. Manage automatic load balancing

Step 1
Step 2
Step 3 etc.

9.1.6.3.2. Manage automatic path failover

Step 1
Step 2
Step 3 etc.

9.1.7 Network Attached Storage Services

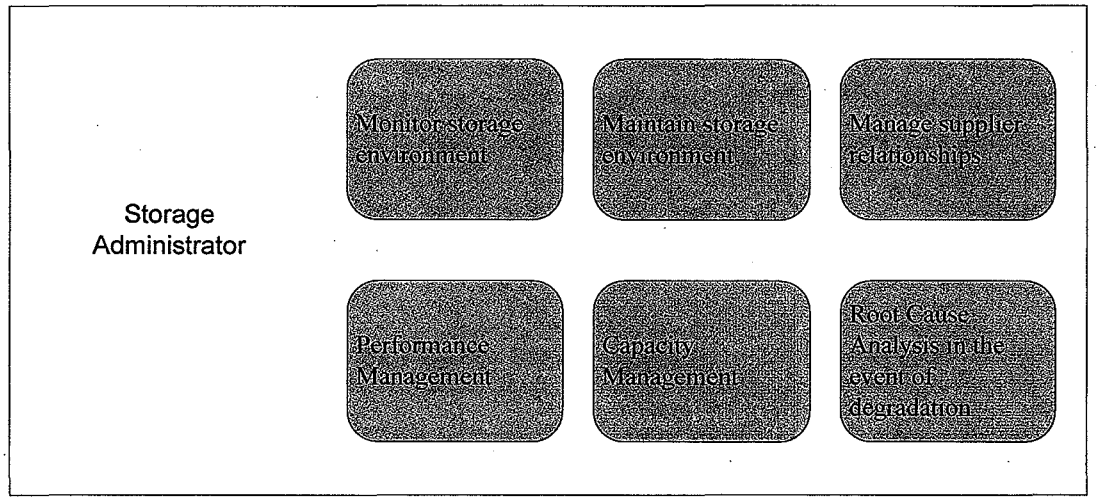
9.1.7.1 Description

Network Attached Storage (NAS) devices located at the Province Managed Storage Facilities, existing at the Hand-Over Date, will be managed by the Service Provider from and after the Hand-Over Date. Network Attached Storage Service is the overall management of the Network Attached Storage (NAS), including monitoring, configuration, control, and tuning software, provided by the Service Provider.

9.1.7.2 How User Requests Services

Type of Request	Method
Minor service requests for Network Attached Storage Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Network Attached Storage Services	Province's iStore system (managed storage requirements definition request)

9.1.7.3 Processes and Procedures



9.1.7.3.1. Monitor storage environment

Step 1
Step 2
Step 3 etc.

9.1.7.3.2. Maintain storage environment

Step 1
Step 2
Step 3 etc.

9.1.7.3.3. Manage supplier relationships

Step 1
Step 2
Step 3 etc.

9.1.7.3.4. Performance management

Step 1
Step 2
Step 3 etc.

9.1.7.3.5. Capacity management

Step 1
Step 2
Step 3 etc.

9.1.7.3.6. Root cause analysis in the event of a degradation

Step 1
Step 2
Step 3 etc.

9.1.8 File System Archive Storage Services (Optional Service)

9.1.8.1 Description

File System Archive ("FSA") is a service that provides automated file movement of Unstructured File Data not under control of a specific application (such as a database or mail messaging) for the purpose of optimizing file storage, managing data growth, and optimizing Backup services by reducing the data volume which is continuously scanned for changes and kept as a copy on Backup media. Data contained in File System Archive will no longer be backed up with Backup Services as there will be two copies of the Data, one in the Calgary Data Centre and one in the Interior Data Centre.

The File Archive Storage function moves the Province's Data from the Source File System to an archival repository. It is a redundant solution that replicates the Province's archive data to a secondary content addressable system for the purpose of extended data protection against component or site failures but is not a Disaster Recovery solution.

Service Provider will only provide an archive storage repository for archival storage requirements other than File Archival Storage including, but not limited to, mail archive or database archive. The Province is responsible for the tools, processes, and people to define the archive policies and extract / retrieve email and other application data.

File Archive automates file movement and retention through Province defined archive software policies and the mirroring of the archive data within the same content addressable system.

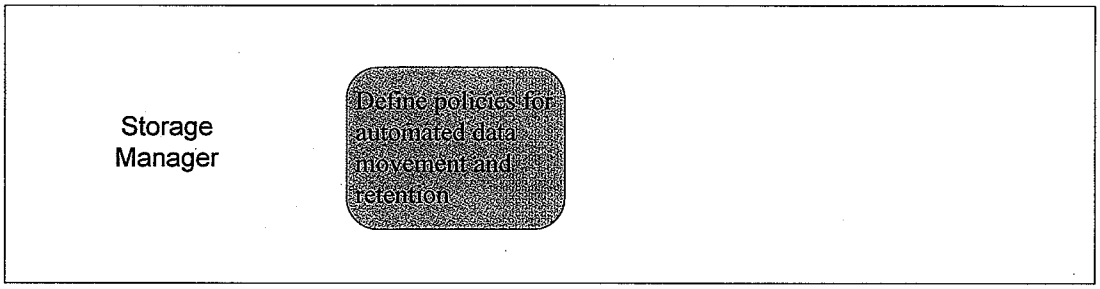
The Managed File Archive solution requires the provisioning of specific Storage Hardware and Storage Software based upon the number of file servers and data volume installed.

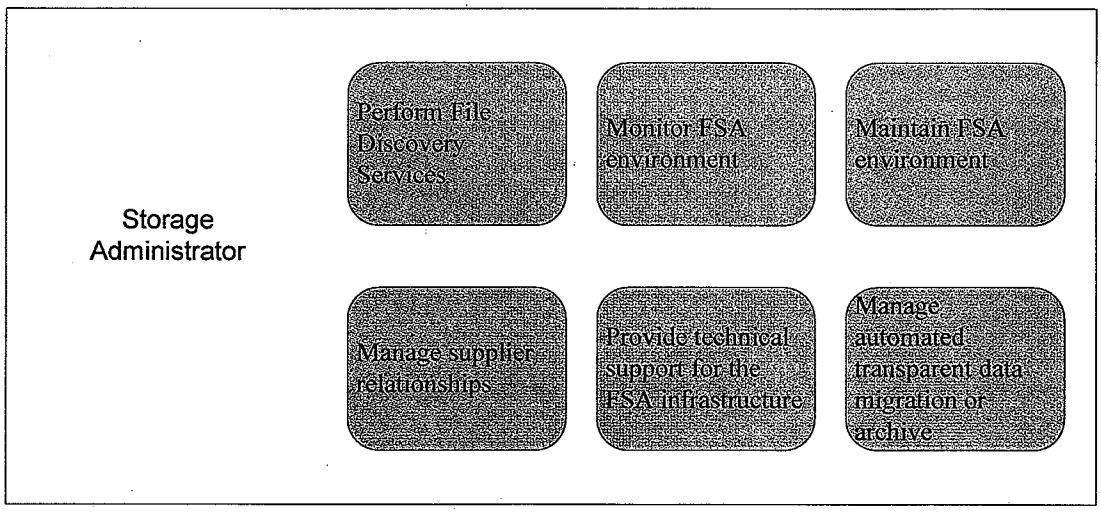
9.1.8.2 How User Requests Services

Type of Request	Method
Minor service requests for File System Archive Storage Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for File System Archive Storage Services	Province's iStore system (managed storage requirements definition request)

Once an assessment of requirements is complete, installation of the File System Archive-related Storage Hardware and Storage Software to be supported can commence. File Discovery Services is then performed on a server-by-server basis to: (i) analyse and report on file structures, (ii) report on usage and/or access of the Province's Data files, and (iii) provide a mechanism for the implementation of the Province's defined policies for the Province's Data file deletion and archiving.

9.1.8.3 Processes and Procedures





9.1.8.3.1. **Define policies for automated data movement and retention**

Step 1
Step 2
Step 3 etc.

9.1.8.3.2. Perform file discovery services

Step 1
Step 2
Step 3 etc.

9.1.8.3.3. Monitor FSA environment

Step 1
Step 2
Step 3 etc.

9.1.8.3.4. Maintain FSA environment

Step 1
Step 2
Step 3 etc.

9.1.8.3.5. Manage supplier relationships

Step 1
Step 2
Step 3 etc.

9.1.8.3.6. Provide technical support for the FSA infrastructure

Step 1
Step 2
Step 3 etc.

9.1.8.3.7. Manage automated transparent data migration or archive

Step 1
Step 2
Step 3 etc.

9.1.9 Configuration Information

The following configuration information is available in Appendix J:

- SAN port connection spreadsheet
- Storage allocation spreadsheet
- Zone configuration report
- Storage array configuration report

9.2 Managed Backup Services

9.2.1 Description

Managed Backup Services is the management of the Backup and restoration of data structured to meet requirements of accessibility, integrity, and recoverability (for example, basic tape-based Backup to disk-based Backup (VTL)). The Service Provider will use integrated Backup Hardware, Backup Software, and services to protect the Data.

The Province will notify the Service Provider, in writing, of the specific servers (at identified locations) and the Data that will receive Backup Services. If specific Data to be backed up is not identified by the Province, as a default position, the Service Provider will back up all Data on such servers. A copy this Data, as requested by the Province, is consolidated on a VTL or tape media to provide the ability to restore the copied Data as requested.

9.2.2 Tape Backup Services

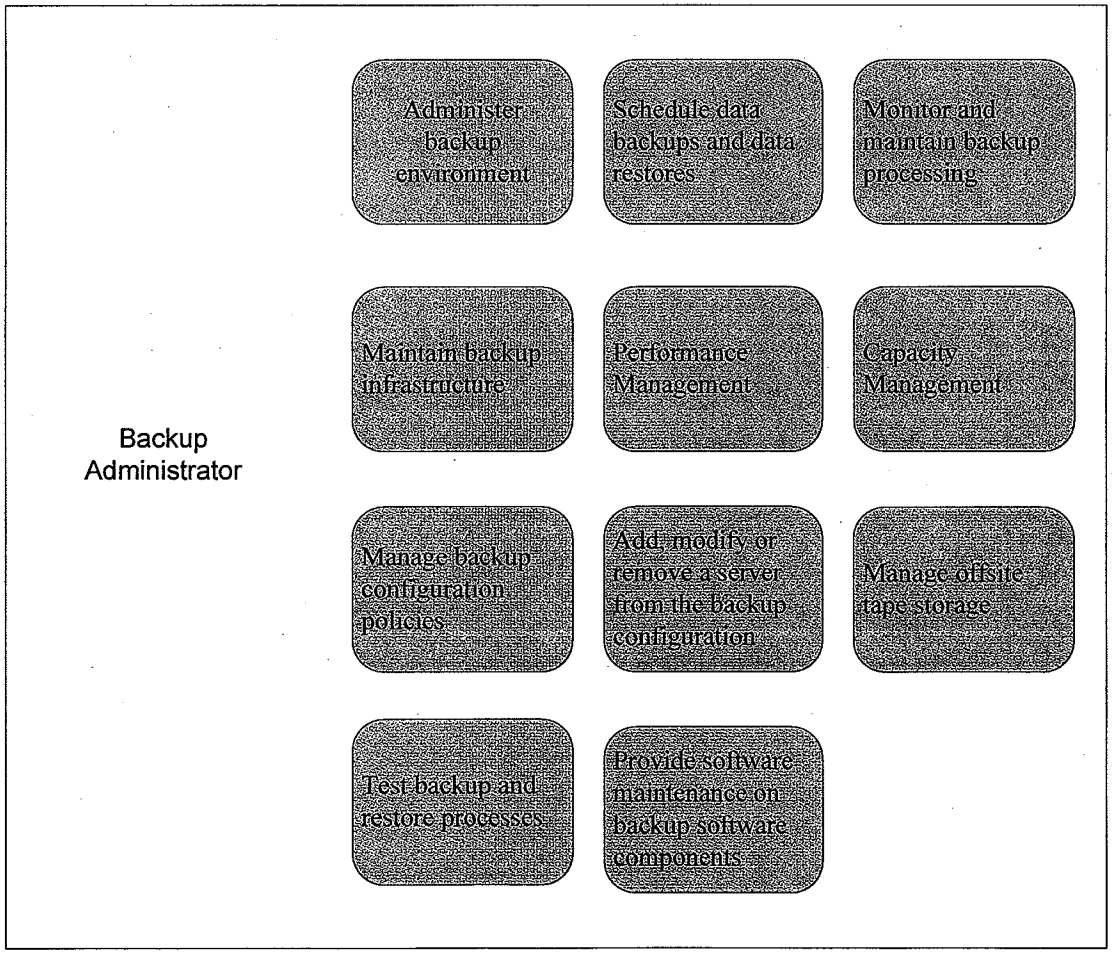
9.2.2.1 Description

Tape Backup Services provides tape based Backup and recovery services for the servers located at the Province Data Centres, Remote Application Server locations and Remote Infrastructure Server locations listed on Schedule 8 (Service Locations) of the MSA. The Service Provider will create a copy of Data, from the primary server, and consolidate and store such Data on a set of magnetic tapes. The Backup of such Data to tape is executed to an offsite location and therefore the tape Backup and originating Data set, located on the primary server, are not in the same physical location.

9.2.2.2 How User Requests Services

Type of Request	Method
Minor service requests for Tape Backup Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Tape Backup Services	Province's iStore system (managed storage requirements definition request)
File backup restore request	WTS Service Desk

9.2.2.3 Processes and Procedures



9.2.2.3.1. Administer backup environment

- Create Backup Procedures
    - Determine which files are critical to restarting a system at any point in time during a systems cycle
    - Determine when these critical files should be backed up
    - Determine which of these critical files should be stored off-site
    - Create procedures that puts these determinations into action
- Create Recovery Procedures
    - Produce a job flow that shows file dependencies by job step
    - Write a description of what steps to follow to restore critical files to an "as of" condition.

9.2.2.3.2. Schedule data backups and data restores

- Schedule data backups
    - Receive user requirements
    - Analyze and validate user requirements
    - Incorporate user requirements into scheduling system
    - Obtain change approval to implement
    - Implement and verify change user scheduling requirements
- Schedule user restores
    - Receive user requirement to restore data
    - Locate media with required data
    - Restore data
    - Confirm data restored to user's satisfaction
    - Close associated restore ticket

9.2.2.3.3. Monitor and maintain backup processing

Step 1
Step 2
Step 3 etc.

9.2.2.3.4. Maintain backup infrastructure

Step 1
Step 2
Step 3 etc.

9.2.2.3.5. Performance management

Step 1
Step 2
Step 3 etc.

9.2.2.3.6. Capacity management

Step 1
Step 2
Step 3 etc.

9.2.2.3.7. Manage backup configuration policy

Step 1
Step 2
Step 3 etc.

9.2.2.3.8. Add, modify or remove a server from the backup configuration

Step 1
Step 2
Step 3 etc.

9.2.2.3.9. Manage offsite tape storage

Step 1
Step 2
Step 3 etc.

9.2.2.3.10. Test backup and restore processes

Step 1
Step 2
Step 3 etc.

9.2.2.3.11. Provide software maintenance on backup software components

Step 1
Step 2
Step 3 etc.

9.2.3 VTL Backup Services with Replication to Secondary Site

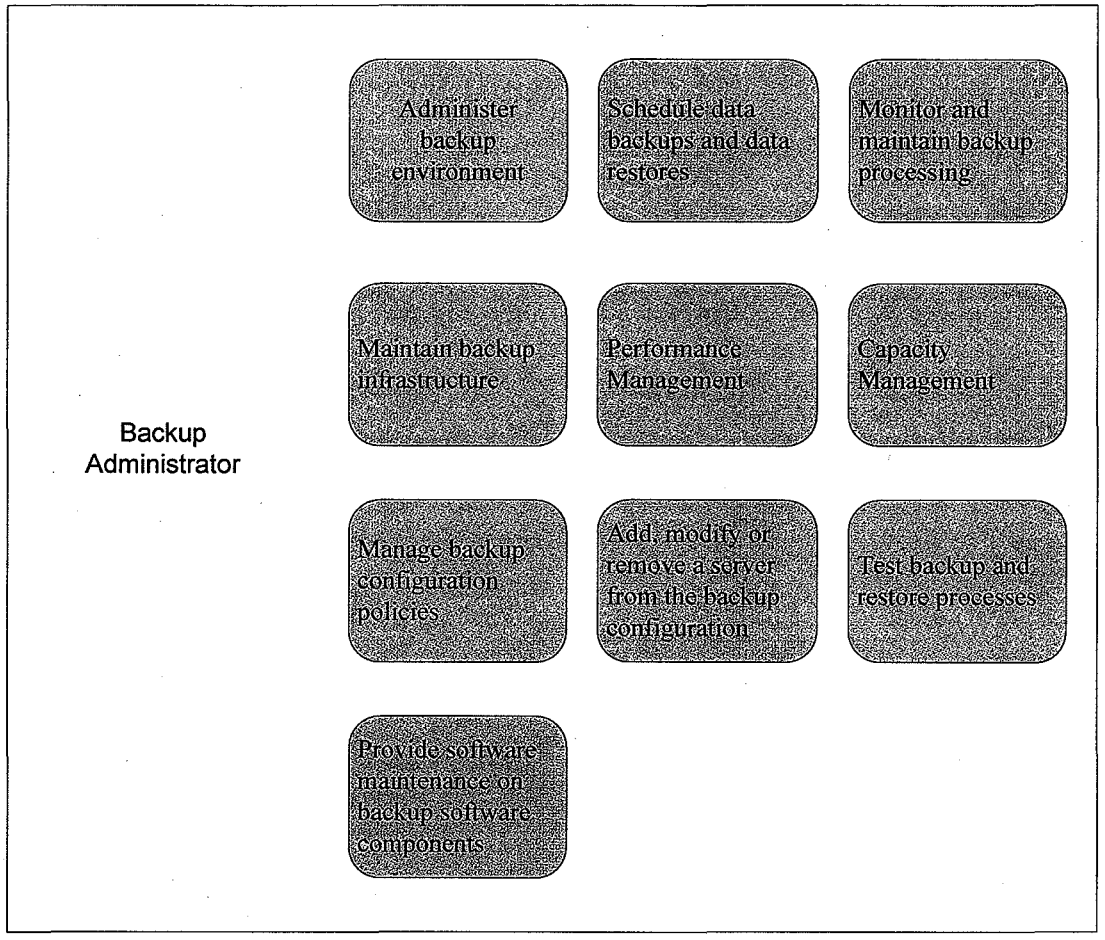
9.2.3.1 Description

VTL Backup Services with Replication to a Secondary Site provides VTL based Backup and recovery services for the servers located at the Service Provider Data Centres listed on Schedule 8 (Service Locations) of the MSA. The Service Provider will Replicate the Data, from the primary server, and consolidate and store a complete Backup set of such Data that is created and retained on Virtual Tapes in a VTL. The Backup Data on the VTL is then Replicated to a second VTL. For example, if the VTL is situated at the Interior Data Centre then the Backup Data will be copied to the secondary VTL situated at the Calgary Data Centre and if the VTL is situated at the Calgary Data Centre then the Backup Data will be copied to the secondary VTL situated at the Interior Data Centre.

9.2.3.2 How User Requests Services

Type of Request	Method
Minor service requests for VTL Backup Services with Replication to a Secondary Site Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for VTL Backup Services with Replication to a Secondary Site Services	Province's iStore system (managed storage requirements definition request)
File backup restore request	WTS Service Desk

9.2.3.3 Processes and Procedures



9.2.3.3.1. Administer backup environment

- Create Backup Procedures
  - Determine which files are critical to restarting a system at any point in time during a systems cycle
  - Determine when these critical files should be backed up
  - Determine which of these critical files should be stored off-site
  - Create procedures that puts these determinations into action
- Create Recovery Procedures
  - Produce a job flow that shows file dependencies by job step
  - Write a description of what steps to follow to restore critical files to an "as of" condition.

9.2.3.3.2. Schedule data backups and data restores

- Schedule data backups
  - Receive user requirements
  - Analyze and validate user requirements
  - Incorporate user requirements into scheduling system

    - Obtain change approval to implement
    - Implement and verify change user scheduling requirements
- Schedule user restores
    - Receive user requirement to restore data
    - Locate media with required data
    - Restore data
    - Confirm data restored to user's satisfaction
    - Close associated restore ticket

9.2.3.3.3. Monitor and maintain backup processing

Step 1
Step 2
Step 3 etc.

9.2.3.3.4. Maintain backup infrastructure

Step 1
Step 2
Step 3 etc.

9.2.3.3.5. Performance management

Step 1
Step 2
Step 3 etc.

9.2.3.3.6. Capacity management

Step 1
Step 2
Step 3 etc.

9.2.3.3.7. Manage backup configuration policy

Step 1
Step 2
Step 3 etc.

9.2.3.3.8. Add, modify or remove a server from the backup configuration

Step 1
Step 2
Step 3 etc.

9.2.3.3.9. Test backup and restore processes

Step 1
Step 2
Step 3 etc.

9.2.3.3.10. Provide software maintenance on backup software components

Step 1
Step 2
Step 3 etc.

9.2.4 VTL Backup to Encrypted Offsite Tape Services (Optional Service)

9.2.4.1 Description

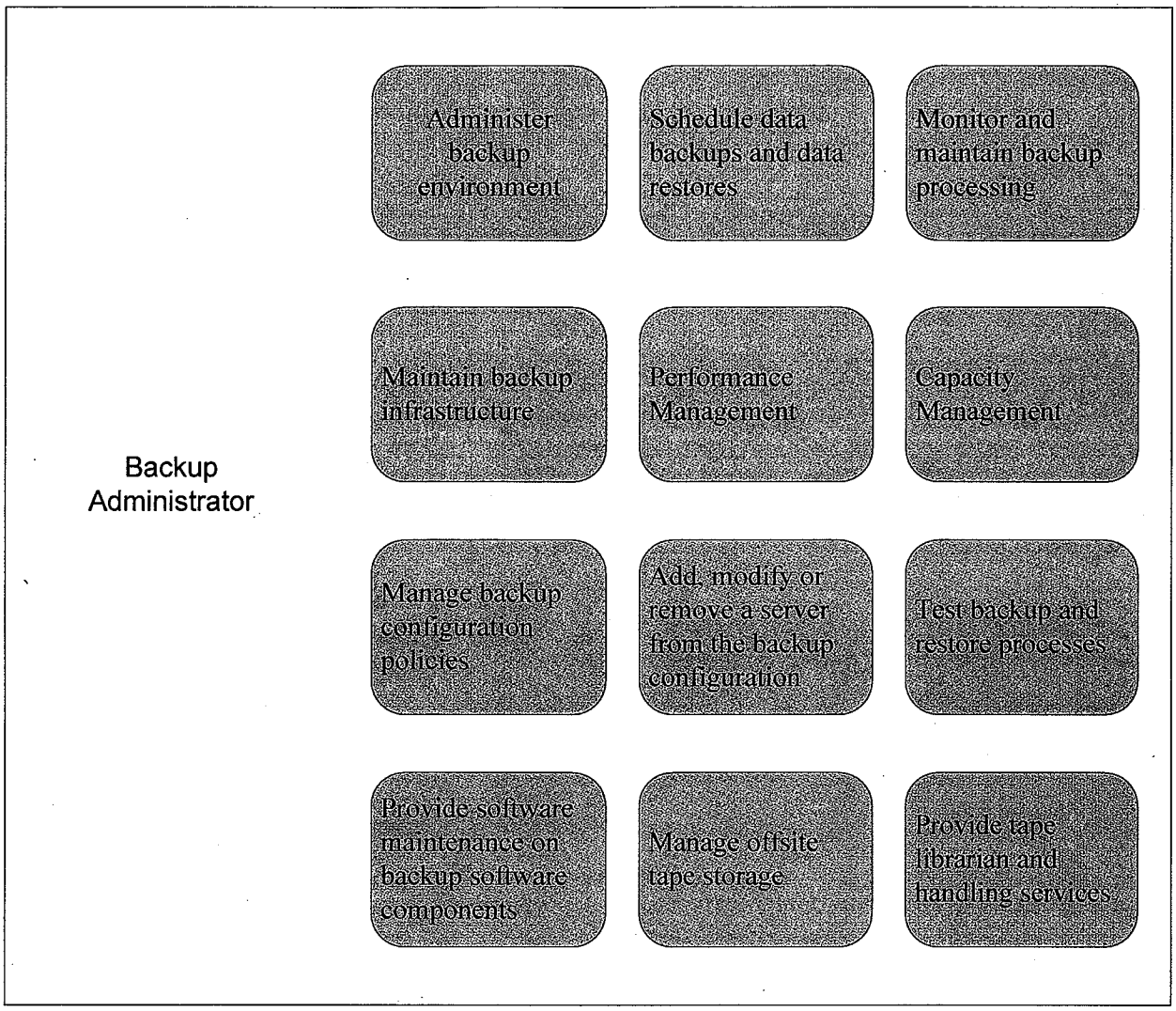
VTL Backup to Encrypted Offsite Tape Service is a VTL to tape based Backup and recovery service for the purpose of facilitating Backup and restore capabilities for Servers located in the Service Provider Data Centres, Remote Application Server locations and Remote Infrastructure Server locations listed on Schedule 8 (Service Locations). Only the current Data Backup resides on the local VTL before being duplicated to and encrypted to tape to be stored at an offsite location. This approach to Data Backup will be used during the period when the Calgary Data Centre is [operational/Service Availability Date] but the Interior Data Centre is not yet [operational/Service Availability Date].

Upon both Service Provider Data Centres becoming [operational/Service Availability Date], the [standard/base/core] Data Backup service will be the VTL Backup Services with Replication to Secondary Site as set forth in section 9.2.3 above. Once both the Service Provider Data Centres are operational, the Province may continue to purchase VTL Backup to Encrypted Offsite Tape Service, as an economy service.

9.2.4.2 How User Requests Services

Type of Request	Method
Minor service requests for VTL Backup to Encrypted Offsite Tape Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for VTL Backup to Encrypted Offsite Tape Services	Province's iStore system (managed storage requirements definition request)
File backup restore request	WTS Service Desk

9.2.4.3 Processes and Procedures



9.2.4.3.1. Administer backup environment

Step 1
Step 2
Step 3 etc.

9.2.4.3.2. Schedule data backups and data restores

Step 1
Step 2
Step 3 etc.

9.2.4.3.3. Monitor and maintain backup processing

Step 1
Step 2
Step 3 etc.

9.2.4.3.4. Maintain backup infrastructure

Step 1

Step 2
Step 3 etc.

9.2.4.3.5. Performance management

Step 1
Step 2
Step 3 etc.

9.2.4.3.6. Capacity management

Step 1
Step 2
Step 3 etc.

9.2.4.3.7. Manage backup configuration policy

Step 1
Step 2
Step 3 etc.

9.2.4.3.8. Add, modify or remove a server from the backup configuration

Step 1
Step 2
Step 3 etc.

9.2.4.3.9. Test backup and restore processes

Step 1
Step 2
Step 3 etc.

9.2.4.3.10. Provide software maintenance on backup software components

Step 1
Step 2
Step 3 etc.

9.2.4.3.11. Manage offsite tape storage

Step 1
Step 2
Step 3 etc.

9.2.4.3.12. Provide tape librarian and handling services

Step 1
Step 2
Step 3 etc.

9.2.5 Extended Retention Period for Tape Services Replication Services

9.2.5.1 Description

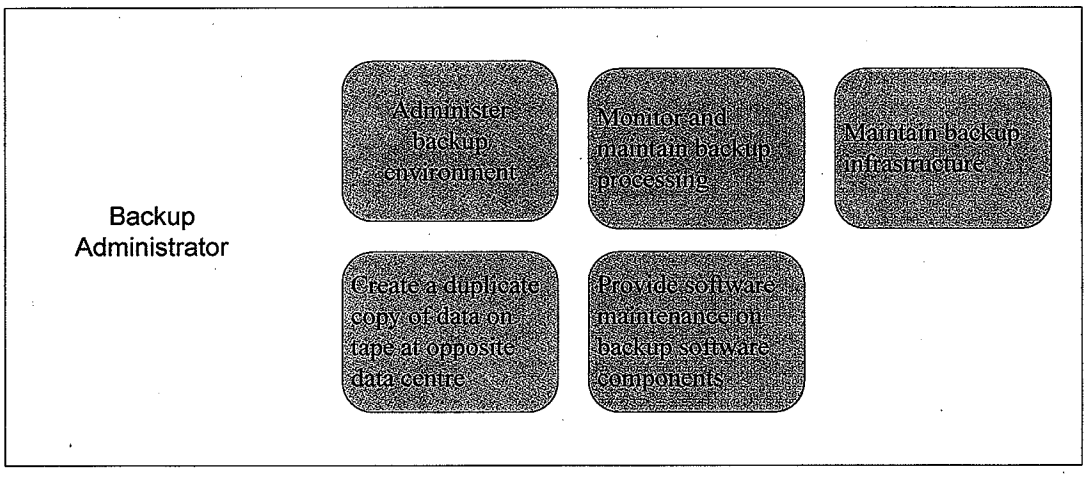
For VTL Backup Services with Replication to a Secondary Site Extended Retention Services, the Province may request that the Data that is backed up be retained for a period of more than ninety (90) days. In which case, the Service Provider will

duplicate a copy of the Data from VTL and write the Data to tape. For Extended Retention Services, if the VTL is situated at the Interior Data Centre then the Backup Data will be copied to the secondary VTL situated at the Calgary Data Centre and then copied to tape (written to onsite tape robot) at the Calgary Data Centre. If the VTL is situated at the Calgary Data Centre then the Backup Data will be copied to the secondary VTL Situated at the Interior Data Centre and then copied to tape (written to onsite tape robot) at the Interior Data Centre.

9.2.5.2 How User Requests Services

Type of Request	Method
Minor service requests for VTL Backup Services with Replication to a Secondary Site Extended Retention Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for VTL Backup Services with Replication to a Secondary Site Extended Retention Services	Province's iStore system (managed storage requirements definition request)

9.2.5.3 Processes and Procedures



9.2.5.3.1. Administer backup environment

Step 1
Step 2
Step 3 etc.

9.2.5.3.2. Monitor and maintain backup processing

Step 1
Step 2
Step 3 etc.

9.2.5.3.3. Maintain backup infrastructure

Step 1
Step 2
Step 3 etc.

9.2.5.3.4. Create a duplicate copy of data on tape at opposite data centre

Step 1

Step 2
Step 3 etc.

9.2.5.3.5. Provide software maintenance on backup software components

Step 1
Step 2
Step 3 etc.

9.2.6 Configuration Information

The following configuration information is available in Appendix L:

- Runbooks describing the scheduling of the backups by CA Workload to the NetBackup server

9.3 Installation, Configuration and Testing Services

9.3.1 Description

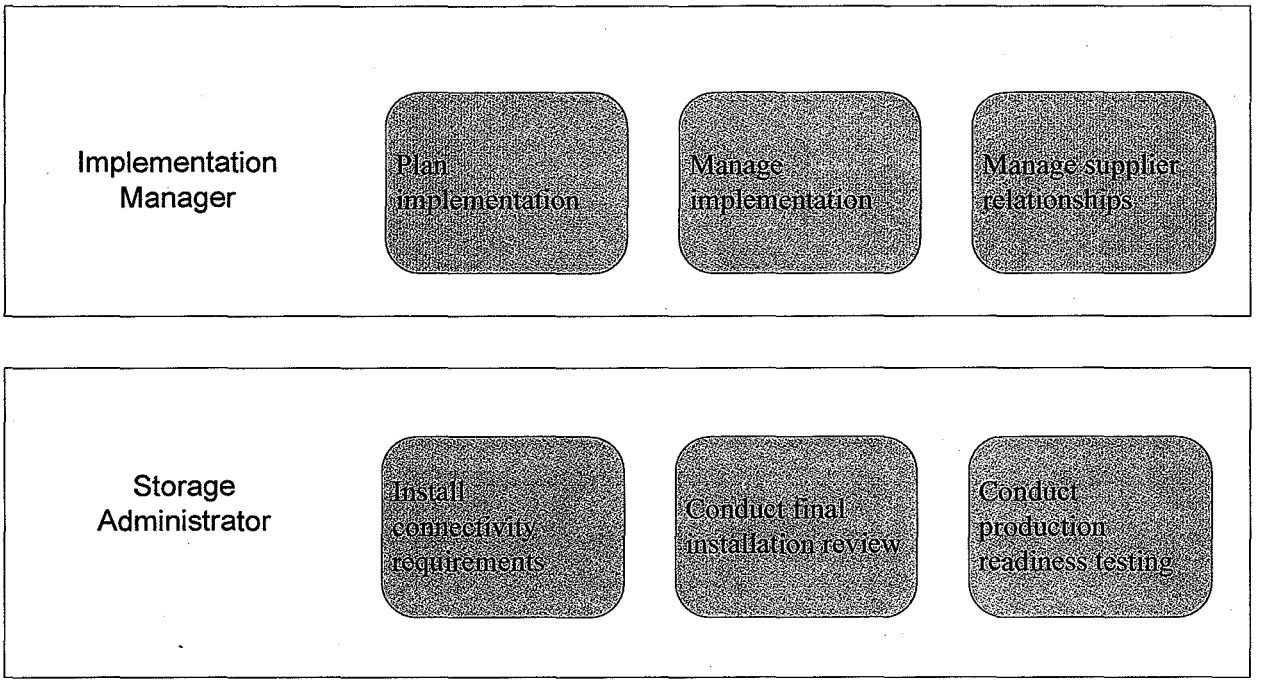
Installation, Configuration and Testing Services for the Province Managed Storage Facilities and Province Managed Backup Facilities is the planning for the any new Storage Hardware, Backup Hardware, Storage Software or Backup Software (due to hardware refresh or to support growth) in the Province Managed Storage Facilities or Province Manage Backup Facilities, and includes installation, configuration, integration and testing services for such new hardware and software. Using the test plan and with support from the Province, Service Provider will validate the connectivity and access to the provincial data centre and test the agreed to services, including the storage and Backup equipment.

Installation, Configuration and Testing Services for the Service Provider Data Centres is the planning for the any new Storage Hardware, Backup Hardware, Storage Software or Backup Software (due to hardware refresh or to support growth) in the Service Provider Data Centres, and includes installation, configuration, integration and testing services for such new Storage Hardware, Backup Hardware, Storage Software or Backup Software.

9.3.2 How User Requests Services

Type of Request	Method
Minor service requests for Installation, Configuration and Testing Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Installation, Configuration and Testing Services	Province's iStore system (managed storage requirements definition request)

9.3.3 Processes and Procedures



9.3.3.1 Plan implementation

Step 1
Step 2
Step 3 etc.

9.3.3.2 Manage implementation

Step 1
Step 2
Step 3 etc.

9.3.3.3 Manage supplier relationships

Step 1
Step 2
Step 3 etc.

9.3.3.4 Install connectivity requirements

Step 1
Step 2
Step 3 etc.

9.3.3.5 Conduct final installation review

Step 1
Step 2
Step 3 etc.

9.3.3.6 Conduct production readiness testing

Step 1
Step 2

Step 3 etc.

9.4 Common Service Delivery

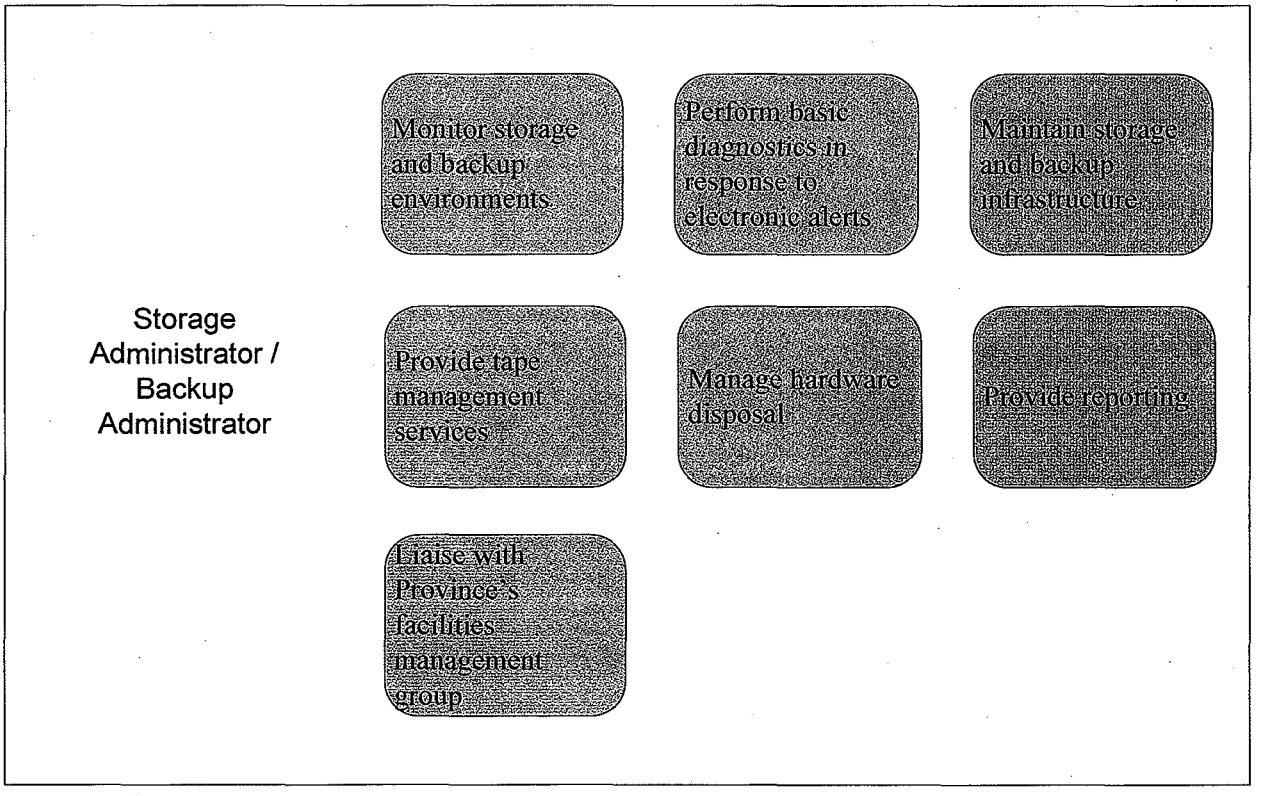
9.4.1 Description

Service Delivery is the operational process required to maintain resource capacity, availability, continuity and committed service levels. Service Provider will provide the following recurring activities: patch management and Storage Hardware, Backup Hardware, Storage Software and Backup Software maintenance of Service Provider managed equipment; and the monitoring of such hardware and software or other recurring activities as agreed to in the Change Management process.

9.4.2 How User Requests Services

Type of Request	Method
Minor service requests for non-automated support such as tape loads, mounts, creation, destruction, retrieval and shipping, returning tapes to the scratch pool, and any other that are within scope of the contracted service	WTS Service Desk (i.e. Priority 6 tickets)
Adhoc support requests	Emails from authorized users to group mailbox

9.4.3 Processes and Procedures



9.4.3.1.1. Monitor storage and backup environments

Step 1

Step 2
Step 3 etc.

9.4.3.1.2. Perform basic diagnostics in response to electronic alerts

Step 1
Step 2
Step 3 etc.

9.4.3.1.3. Maintain storage and backup infrastructure

Step 1
Step 2
Step 3 etc.

9.4.3.1.4. Provide tape management services

Step 1
Step 2
Step 3 etc.

9.4.3.1.5. Manage hardware disposal

Step 1
Step 2
Step 3 etc.

9.4.3.1.6. Provide reporting

Step 1
Step 2
Step 3 etc.

9.4.3.1.7. Liaise with Province's facilities management group

Step 1
Step 2
Step 3 etc.

9.5 Storage Connectivity Services

9.5.1 Description

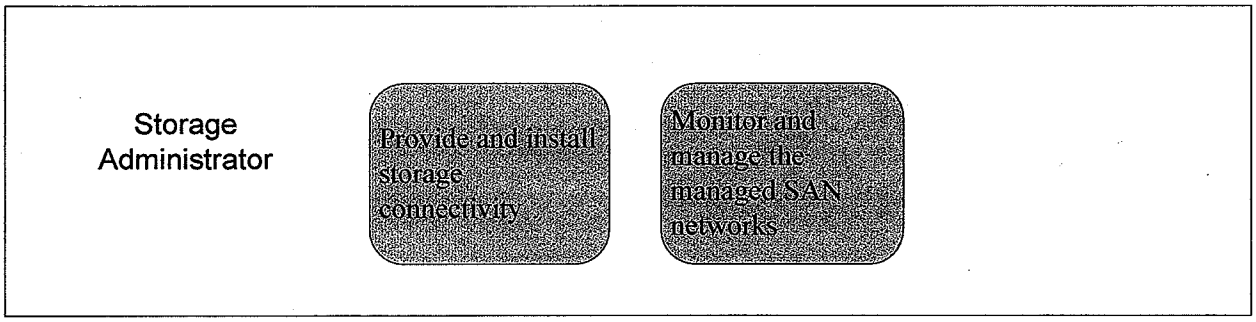
Storage Connectivity Services is the management of the connectivity equipment (such as switches, fibre cables) that connect Storage Arrays and Tape Libraries to Servers in such a way that the Storage LUN's and Tape Drives appear as though they are locally attached to the Server.

9.5.2 How User Requests Services

Type of Request	Method
Minor service requests for Storage Connectivity Services	WTS Service Desk (i.e. Priority 6 tickets)
Formal requests for Storage Connectivity Services	Province's iStore system (managed storage requirements definition request)

Adhoc requests	Emails from authorized users to group mailbox

9.5.3 Processes and Procedures



9.5.3.1.1. Perform and install storage connectivity

Step 1
Step 2
Step 3 etc.

9.5.3.1.2. Monitor and manage the managed SAN networks

Step 1
Step 2
Step 3 etc.

9.5.4 Configuration Information

A connectivity diagram showing the connections between Storage Arrays, Tape Libraries and Servers may be found in Appendix J.

16.1 Description

16.2 Process Deliverables

16.3 Processes and Procedures

16.4 Tools

16.5 Communications

APPENDIX A - GLOSSARY OF TERMS AND DEFINITIONS

APPENDIX B - FORMS

APPENDIX C - RELATIONSHIPS AND AUTHORIZED CONTACTS

APPENDIX D - SUPPORTED SITES

APPENDIX E - NETWORK CONFIGURATION AND DIAGRAMS

APPENDIX F - MAINFRAME CONFIGURATION

APPENDIX G - SERVER CONFIGURATIONS

APPENDIX H - SUPPORTED SERVERS

APPENDIX I - STANDARD SOFTWARE

APPENDIX J - STORAGE CONFIGURATIONS

SAN Port Connection Spreadsheet and Storage Allocation Spreadsheet

SAMPLE SAN
PORT CONNECTIC

Zone Configuration Report

SAN
_FABRIC_ZONE C(

Storage Array Configuration Report

EVA
CONFIGURATION

Connectivity Diagram

N/A

APPENDIX K - TAPE HANDLING PROCESS

APPENDIX L – SAMPLE BACKUP RUNBOOK

BUR Demo
Runbook.doc

APPENDIX M - ESCALATION TIME LINES

APPENDIX N - SCHEDULED MAINTENANCE CHANGE WINDOWS

APPENDIX O - JOB SCHEDULING PROCEDURES

APPENDIX P - MEETING SCHEDULES

APPENDIX Q - CHANGE REQUEST FORMS

APPENDIX R - SECURITY FORMS

APPENDIX S - VOLUMETRICS

APPENDIX T - PROVINCE ORGANIZATION CHART

Appendix D - Province Freeze Periods

This table represents the periods during which the Province has designated restrictions on changes to their Applications, as identified, during the first three years of the term of the Agreement. It is the intent of the Parties that these constraints are considered during the initial refinement of the Transformation Plan and that any conflicts are resolved by the Parties before the plan is approved.

S15

S15 This constraint will also be considered during the initial refinement of the Transformation Plan and conflicts will be resolved by the Parties before the plan is approved including the scheduling of the Mainframe Service Migration fo S15

Client	Hosting Freeze Conditions	Platform	Freeze Timeframes
			At issue for Inquiry
		UNIX	
		Windows	
		UNIX	
		Windows	
		UNIX (co-lo hosting)	
		MVS	
	S15		
		Windows	S15
		MVS	
		OpenVMS	
		Windows	

Client	Hosting Freeze Conditions	Platform	Freeze Timeframes
		OpenVMS	
		Windows UNIX	
		Windows UNIX MVS OpenVMS	
		Windows UNIX	
		UNIX Windows	
	S15	Windows VMWare	S15
		Windows UNIX	
		MVS	
		MVS	
		Windows UNIX	
		Windows UNIX	

Client	Hosting Freeze Conditions	Platform	Freeze Timeframes
S15		MVS	S15
		Windows UNIX MVS	
		MVS	
		MVS	
		UNIX Windows	
		Windows UNIX MVS VMWare	
		MVS	
		Windows MVS	
		UNIX	

Client	Hosting Freeze Conditions	Platform	Freeze Timeframes
		UNIX	
		Windows MVS	
		UNIX MVS	
	S15		S15
		Windows	
		Windows UNIX	
		Windows UNIX	

Appendix E – Milestone (see table above) Deliverable Certification

See attached.

At issue for Inquiry

S. 15

S. 15

At issue for Inquiry

SCHEDULE 10

TRANSFORMATION PLAN

See attached.

SCHEDULE 10 – TRANSFORMATION PLAN

Table of Contents

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
1	NA	**V0.8.4 STMS Schedule 10 - Transformation Plan**	**Fri 05 Sep '08**	**1460 days?**	**Mon 31 Mar '14**		
2							
3	NA	**Key Dates**	**Mon 30 Mar '09**	**574 days**	**Tue 31 May '11**		
4	Mon 30 Mar '09	Contract Sign	Mon 30 Mar '09	0 days	Mon 30 Mar '09		
5	Mon 30 Mar '09	Hand-Over Date	Mon 30 Mar '09	0 days	Mon 30 Mar '09		
6	NA	SP Office Facility ready for staff	Mon 01 Jun '09	0 days	Mon 01 Jun '09	44	
7	NA	SP Service Management Tool and Process Go Live	Sun 27 Sep '09	0 days	Sun 27 Sep '09	240	
8	NA	STMS Calgary Data Centre Availability Date (for SP set-up)	Sun 01 Nov '09	0 days	Sun 01 Nov '09	57	
9	NA	STMS Calgary Data Centre Ready for Production Operations	Thu 31 Dec '09	0 days	Thu 31 Dec '09	163,471	
10	NA	Mainframe Services Migration Date	Sun 02 Jan '11	0 days	Sun 02 Jan '11	285	
11	NA	STMS Interior Data Centre Availability Date (for SP setup)	Fri 01 Apr '11	0 days	Fri 01 Apr '11	81	
12	NA	STMS Interior Data Centre Ready for Production Operations	Tue 31 May '11	0 days	Tue 31 May '11	186,487	
13	NA	**Service Provider Business Operations Implementation**	**Mon 30 Mar '09**	**138 days**	**Thu 01 Oct '09**		
14	NA	**Establish Programme Office**	**Mon 30 Mar '09**	**138 days**	**Thu 01 Oct '09**		
15	NA	Implement at Service Provider Governance Processes described in Agreement	Mon 30 Mar '09	25 days	Thu 30 Apr '09	5	SP
16	NA	Implement project issues, risk management tool & process	Mon 30 Mar '09	25 days	Thu 30 Apr '09	5	SP
17	NA	Establish Transformation Project status reporting	Mon 30 Mar '09	25 days	Thu 30 Apr '09	5	SP
18	NA	Implement SLA Reporting for CMO	Mon 30 Mar '09	25 days	Thu 30 Apr '09	5	SP
19	NA	**Establish FMO SLA Reporting**	**Mon 30 Mar '09**	**138 days**	**Thu 01 Oct '09**		
20	NA	Determine source of SLA reporting data for FMO	Mon 30 Mar '09	46 days	Fri 29 May '09	5	SP
21	NA	Develop process to collect SLA metrics	Mon 01 Jun '09	46 days	Thu 30 Jul '09	20	SP
22	NA	Implement SLA Reporting capability for FMO	Fri 31 Jul '09	46 days	Thu 01 Oct '09	21	SP
23	NA	**Establish Business Office**	**Mon 30 Mar '09**	**138 days**	**Thu 01 Oct '09**		
24	NA	Obtain approval for early procurement of Opsware and CA hardware and software	Mon 30 Mar '09	1 day	Mon 30 Mar '09	4	SP
25	NA	Obtain approval to procure hardware/software (CAN)	Mon 30 Mar '09	4 days	Thu 02 Apr '09	5	SP
26	NA	Complete Financial Mgmt Start- up (includes CMO billing capability)	Mon 30 Mar '09	25 days	Thu 30 Apr '09	5	SP
27	NA	Business Office Staffed and Operational	Thu 30 Apr '09	0 days	Thu 30 Apr '09	26,18	SP
28	NA	**Establish FMO billing capability**	**Mon 30 Mar '09**	**138 days**	**Thu 01 Oct '09**		
29	NA	Determine source of billing data	Mon 30 Mar '09	38 days	Tue 19 May '09	5	SP
30	NA	Develop process to collect billing data	Wed 20 May '09	54 days	Thu 30 Jul '09	29	SP
31	NA	Implement steady state FMO billing capability	Fri 31 Jul '09	46 days	Thu 01 Oct '09	30	SP
32	NA	**Implement Client Care Processes**	**Mon 30 Mar '09**	**25 days**	**Thu 30 Apr '09**		
33	NA	Implement initial internal Service Provider Communication Plan	Mon 30 Mar '09	25 days	Thu 30 Apr '09	5	SP
34	NA	Prepare and Implement initial Service Provider to Province Communication Plan	Mon 30 Mar '09	25 days	Thu 30 Apr '09	33SS	Prov
35	NA	Prepare and Implement Initial Service Provider to Province Communication Plan	Mon 30 Mar '09	25 days	Thu 30 Apr '09	33SS	SP
36	NA	**Refine Transformation Plan**	**Mon 30 Mar '09**	**61 days**	**Fri 19 Jun '09**		
37	NA	Develop Initial Refinement of Transformation Plan	Mon 30 Mar '09	46 days	Fri 29 May '09	5	SP
38	NA	Design Storyboard Session to Review Proposed Refinements of Transformation Plan	Mon 01 Jun '09	5 days	Fri 05 Jun '09	37	SP
39	NA	Approve Initial Refinement of Transformation Plan	Mon 08 Jun '09	10 days	Fri 19 Jun '09	38	SP
40	NA	Approve Initial Refinment of Transformation Plan	Mon 08 Jun '09	10 days	Fri 19 Jun '09	39SS	Prov
41	NA	**Office Facilities Transformation**	**Mon 30 Mar '09**	**70 days**	**Tue 30 Jun '09**		
42	NA	Order COE Equipment for Staff	Fri 03 Apr '09	5 days	Thu 09 Apr '09	25	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
43	NA	Order MOS Equipment for Office Facility	Fri 03 Apr '09	5 days	Thu 09 Apr '09	25	SP
44	NA	Preparation of Office Facilities (at VITP)	Mon 30 Mar '09	47 days	Mon 01 Jun '09	4	SP
45	Tue 02 Jun '09	SP exit from WTS Office Facilities (move from Seymour to VITP)	Tue 02 Jun '09	23 days	Tue 30 Jun '09	44	SP
46	NA	**Data Centre Facilities Transformation**	**Fri 05 Sep '08**	**721 days?**	**Tue 31 May '11**		
47	NA	**STMS Calgary Data Centre Build Out**	**Tue 05 May '09**	**218 days**	**Fri 26 Feb '10**		
48	NA	**Construction Progress Reporting**	**Mon 15 Jun '09**	**91 days**	**Thu 15 Oct '09**		
49	Mon 15 Jun '09	Major Equipment Installation Nearing Completion (date to be confirmed)	Mon 15 Jun '09	0 days	Mon 15 Jun '09		SP
50	Sat 15 Aug '09	Start Commissioning Major Equipment (date to be confirmed)	Sat 15 Aug '09	0 days	Sat 15 Aug '09		SP
51	Tue 15 Sep '09	Commissioning substantially comple (date to be confirmed)	Tue 15 Sep '09	0 days	Tue 15 Sep '09		SP
52	Thu 15 Oct '09	Project complete, ready for customer to move in (date to be confirmed)	Thu 15 Oct '09	0 days	Thu 15 Oct '09		SP
53	NA	Design SP Managed Services Cage	Tue 05 May '09	20 days	Mon 01 Jun '09	55SS-66 days	SP
54	Tue 30 Jun '09	Revised Initial VA capacity reservation	Tue 30 Jun '09	0 days	Tue 30 Jun '09		Prov
55	NA	Final Calgary cage design completed and accepted by SP	Sat 01 Aug '09	10 days	Thu 13 Aug '09	57SS-66 days	SP
56	NA	Builds Initial Cage, Wiring Trays & Installs Racks	Mon 05 Oct '09	20 days	Sun 01 Nov '09	57FF	SP
57	Sun 01 Nov '09	STMS Calgary Data Centre Availability Date (for SP set-up)	Sun 01 Nov '09	0 days	Sun 01 Nov '09		SP
58	NA	Conduct Security Threat and Risk Assessment	Sun 01 Nov '09	20 days	Thu 26 Nov '09	57	SP
59	NA	STMS Calgary Data Centre Ready for Production Operations	Thu 31 Dec '09	0 days	Thu 31 Dec '09	163,471	SP
60	Mon 22 Feb '10	STMS Calgary Data Centre Requirements Verification	Mon 22 Feb '10	5 days	Fri 26 Feb '10		SP
61	NA	**STMS Interior Data Centre Build Out**	**Fri 05 Sep '08**	**721 days?**	**Tue 31 May '11**		
62	Wed 15 Apr '09	Completion of Purchase (Milestone description to be confirmed)	Wed 15 Apr '09	0 days	Wed 15 Apr '09		SP
63	NA	Construction Progress Reporting (to be confirmed)	Mon 15 Jun '09	421 days?	Sat 15 Jan '11		S{
64	Mon 15 Jun '09	Conceptual Design Complete (date to be confirmed)	Mon 15 Jun '09	0 days	Mon 15 Jun '09		SP
65	Mon 15 Jun '09	Earthworks (date to be confirmed)	Mon 15 Jun '09	0 days	Mon 15 Jun '09		SP
66	Sat 15 Aug '09	Building permits issued (date to be confirmed)	Sat 15 Aug '09	0 days	Sat 15 Aug '09		SP
67	Thu 15 Oct '09	Structural steel work (date to be confirmed)	Thu 15 Oct '09	0 days	Thu 15 Oct '09		SP
68	Tue 15 Dec '09	Structural Framing complete (date to be confirmed)	Tue 15 Dec '09	0 days	Tue 15 Dec '09		SP
69	Mon 15 Feb '10	Building Shell and Roof Complete (date to be confirmed)	Mon 15 Feb '10	0 days	Mon 15 Feb '10		SP
70	Thu 15 Apr '10	Major equipment on SIte (date to be confirmed)	Thu 15 Apr '10	1 day?	Thu 15 Apr '10		SP
71	Tue 15 Jun '10	Major Equipment Placed (date to be confirmed)	Tue 15 Jun '10	1 day?	Tue 15 Jun '10		SP
72	Sun 15 Aug '10	Major equipment installation nearing completion (date to be confirmed)	Mon 16 Aug '10	1 day?	Mon 16 Aug '10		SP
73	Fri 15 Oct '10	Start Commissioning Major Equipment (date to be confirmed)	Fri 15 Oct '10	0 days	Fri 15 Oct '10		SP
74	Mon 15 Nov '10	Commissioning substantially comple (date to be confirmed)	Mon 15 Nov '10	0 days	Mon 15 Nov '10		SP
75	Sat 15 Jan '11	Project complete, ready for customer to move in (date to be confirmed)	Sat 15 Jan '11	0 days	Sat 15 Jan '11		SP
76	Tue 30 Jun '09	Revised Initial VA capacity reservation	Tue 30 Jun '09	0 days	Tue 30 Jun '09		Prov
77	NA	Design SP Managed Services Cage	Fri 01 Oct '10	20 days	Thu 28 Oct '10	79SS-66 days	SP
78	NA	Design Co-location Cages For BPS	Fri 05 Sep '08	20 days	Thu 02 Oct '08		SP
79	NA	Final Calgary cage design completed and accepted by SP	Sat 01 Jan '11	10 days	Wed 12 Jan '11	81SS-66 days	SP
80	NA	Builds Initial Cage, Wiring Trays & Installs Racks	Fri 04 Mar '11	20 days	Fri 01 Apr '11	81FF	SP
81	Fri 01 Apr '11	STMS Interior Data Centre Availability Date (for SP set-up)	Fri 01 Apr '11	0 days	Fri 01 Apr '11		SP
82	NA	Conduct Security Threat and Risk Assessment	Fri 01 Apr '11	20 days	Thu 28 Apr '11	81	SP
83	NA	STMS Interior Data Centre Ready for Production Operations	Tue 31 May '11	0 days	Tue 31 May '11	186,487	SP
84	Mon 22 Jun '09	STMS Interior Data Centre Requirements Verification	Mon 22 Jun '09	5 days	Fri 26 Jun '09		SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
85	NA	**Network (LAN/WAN) Transformation**	**Mon 15 Dec '08**	**635 days**	**Tue 10 May '11**		
86	NA	**Install Management Network Project**	**Mon 15 Dec '08**	**155 days**	**Mon 13 Jul '09**		
87	NA	**Early circuit order to relieve Mid-Range critical path**	**Mon 15 Dec '08**	**78 days**	**Tue 31 Mar '09**		
88	Mon 15 Dec '08	Submit ICAR for early circuit order	Mon 15 Dec '08	1 day	Mon 15 Dec '08		SP
89	NA	**Prepare Design Proposal Summary**	**Tue 16 Dec '08**	**11 days**	**Tue 30 Dec '08**		
90	NA	S15 Site Firewalls	Tue 16 Dec '08	3 days	Thu 18 Dec '08	88	SP
91	NA	SDN Connectivity	Fri 19 Dec '08	4 days	Wed 24 Dec '08	90	SP
92	NA	WAN Connectivity	Thu 25 Dec '08	3 days	Mon 29 Dec '08	91	SP
93	NA	Sign-off of DPS	Tue 30 Dec '08	1 day	Tue 30 Dec '08	92	SP
94	Mon 05 Jan '09	Early circuit order	Mon 05 Jan '09	1 day	Mon 05 Jan '09		SP
95	NA	Early hardware order	Mon 05 Jan '09	1 day	Mon 05 Jan '09	94SS	SP
96	NA	Request to Province for third party gateway firewall preparations	Mon 05 Jan '09	1 day	Mon 05 Jan '09	94SS	SP
97	NA	Install and configure third party gateway firewall	Tue 06 Jan '09	50 days	Fri 13 Mar '09	96	Prov
98	NA	Support installation and configuration of third party firewall gateway	Tue 06 Jan '09	50 days	Fri 13 Mar '09	97SS	SP
99	NA	early circuit terminations completed by carrier	Fri 13 Mar '09	0 days	Fri 13 Mar '09	98	SP
100	NA	Test connectivity	Mon 30 Mar '09	2 days	Tue 31 Mar '09	5	Prov
101	NA	Test connectivity	Mon 30 Mar '09	2 days	Tue 31 Mar '09	5	SP
102	NA	Early circuit for initial connect of management network ready to use	Tue 31 Mar '09	0 days	Tue 31 Mar '09	101	SP
103	NA	**Balance of Management Network Install to achieve full capacity**	**Mon 30 Mar '09**	**79 days**	**Mon 13 Jul '09**		
104	NA	**Prepare Design Proposal Summary**	**Mon 30 Mar '09**	**11 days**	**Mon 13 Apr '09**		
105	NA	S15 Site Firewalls	Mon 30 Mar '09	3 days	Wed 01 Apr '09	5SS	SP
106	NA	SDN Connectivity	Thu 02 Apr '09	4 days	Tue 07 Apr '09	105	SP
107	NA	WAN Connectivity	Wed 08 Apr '09	3 days	Fri 10 Apr '09	106	SP
108	NA	Sign-off of DPS	Mon 13 Apr '09	1 day	Mon 13 Apr '09	107	SP
109	NA	Order circuits	Tue 14 Apr '09	45 days	Fri 12 Jun '09	108	SP
110	NA	Order hardware	Tue 14 Apr '09	24 days	Thu 14 May '09	108	SP
111	NA	Request to Province for third party gateway firewall preparations	Tue 14 Apr '09	2 days	Wed 15 Apr '09	108	SP
112	NA	**Install & configure**	**Mon 15 Jun '09**	**23 days**	**Mon 13 Jul '09**		
113	NA	S15 Firewalls	Mon 15 Jun '09	7 days	Sun 21 Jun '09	109,110	SP
114	NA	SDN (Service Delivery Network)	Mon 22 Jun '09	7 days	Tue 30 Jun '09	113	SP
115	NA	WAN - routers carrier	Wed 01 Jul '09	8 days	Fri 10 Jul '09	114	SP
116	NA	Install & Configure Complete	Mon 13 Jul '09	1 day	Mon 13 Jul '09	115	SP
117	NA	Design third party gateway to support connection of management network	Thu 16 Apr '09	23 days	Fri 15 May '09	111	Prov
118	NA	Sign-off on engineering design by SP	Mon 18 May '09	2 days	Tue 19 May '09	117	SP
119	NA	Sign-off on engineering design by Province	Mon 18 May '09	2 days	Tue 19 May '09	117	Prov
120	NA	Procure hardware and software	Wed 20 May '09	14 days	Mon 08 Jun '09	119,118	SP
121	NA	Procure hardware and software	Wed 20 May '09	14 days	Mon 08 Jun '09	120SS	Prov
122	NA	Install and configure 3rd party gateway firewalls	Tue 09 Jun '09	13 days	Tue 23 Jun '09	121,120	Prov
123	NA	Support 3rd party gateway firewall installs	Tue 09 Jun '09	13 days	Tue 23 Jun '09	122SS	SP
124	NA	Test connectivity	Wed 24 Jun '09	5 days	Tue 30 Jun '09	122,109,110	SP
125	NA	Support SP with connectivity test	Wed 24 Jun '09	5 days	Tue 30 Jun '09	124SS	Prov
126	NA	Management Network Complete	Mon 13 Jul '09	0 days	Mon 13 Jul '09	125,116	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
127	NA	**Design & Engineer STMS Data Centre Networks (LAN & WAN)**	**Mon 20 Apr '09**	**408 days**	**Thu 04 Nov '10**		
128	Mon 20 Apr '09	Submit ICAR	Mon 20 Apr '09	1 day	Mon 20 Apr '09		SP
129	NA	Assemble Engineer Team	Tue 21 Apr '09	1 day	Tue 21 Apr '09	128	SP
130	NA	Review and Confirm High Level Design	Wed 22 Apr '09	1 day	Wed 22 Apr '09	129	SP
131	NA	**Prepare Design Proposal - Calgary DC**	**Thu 23 Apr '09**	**33 days**	**Mon 08 Jun '09**		
132	NA	Firewall Detailed Design	Thu 23 Apr '09	8 days	Mon 04 May '09	130	SP
133	NA	IPS Detailed Design	Tue 05 May '09	8 days	Thu 14 May '09	132	SP
134	NA	LAN Detailed Design	Fri 15 May '09	8 days	Tue 26 May '09	133	SP
135	NA	WAN Detailed Design	Wed 27 May '09	8 days	Fri 05 Jun '09	134	SP
136	NA	Sign-off of DPS	Mon 08 Jun '09	1 day	Mon 08 Jun '09	135	SP
137	NA	**Prepare Design Proposal - Interior DC**	**Tue 21 Sep '10**	**33 days**	**Thu 04 Nov '10**		
138	NA	Firewall Detailed Design	Tue 21 Sep '10	8 days	Thu 30 Sep '10	130,81FF-132 days	SP
139	NA	IPS Detailed Design	Fri 01 Oct '10	8 days	Tue 12 Oct '10	138	SP
140	NA	LAN Detailed Design	Wed 13 Oct '10	8 days	Fri 22 Oct '10	139	SP
141	NA	WAN Detailed Design	Mon 25 Oct '10	8 days	Wed 03 Nov '10	140	SP
142	NA	Sign-off of DPS	Thu 04 Nov '10	1 day	Thu 04 Nov '10	141	SP
143	NA	**Install STMS Calgary Data Centre Networks (LAN & WAN) Project**	**Mon 08 Jun '09**	**135 days**	**Tue 08 Dec '09**		
144	NA	**Ordering**	**Mon 08 Jun '09**	**57 days**	**Fri 21 Aug '09**		
145	NA	Order circuits	Mon 08 Jun '09	0 days	Mon 08 Jun '09	25,136	Prov
146	NA	Order hardware	Mon 08 Jun '09	0 days	Mon 08 Jun '09	25,136	SP
147	NA	Hardware received at an alternate SP location	Fri 21 Aug '09	0 days	Fri 21 Aug '09	146FS+57 days	SP
148	NA	**Configure Equipment (at an alternate SP location)**	**Mon 24 Aug '09**	**50 days**	**Fri 30 Oct '09**		
149	NA	Configure LAN core Switches	Mon 24 Aug '09	8 wks	Fri 16 Oct '09	147	SP
150	NA	Configure LAN TOR Switches	Mon 24 Aug '09	8 wks	Fri 16 Oct '09	149SS	SP
151	NA	Configure Firewalls	Mon 24 Aug '09	8 wks	Fri 16 Oct '09	149SS	SP
152	NA	Configure IPS	Mon 24 Aug '09	8 wks	Fri 16 Oct '09	149SS	SP
153	NA	Configure WAN	Mon 24 Aug '09	8 wks	Fri 16 Oct '09	149SS	SP
154	NA	Ship configured equipment to Calgary DC	Mon 19 Oct '09	10 days	Fri 30 Oct '09	153,149,150,151,152	SP
155	NA	**Install Equipment (WAS: Install & Configure)**	**Sun 01 Nov '09**	**18 days**	**Tue 24 Nov '09**		
156	NA	Install LAN core Switches	Sun 01 Nov '09	3 days	Tue 03 Nov '09	57,154	SP
157	NA	Install LAN TOR Switches	Wed 04 Nov '09	3 days	Fri 06 Nov '09	156	SP
158	NA	Install Firewalls	Mon 09 Nov '09	3 days	Wed 11 Nov '09	157	SP
159	NA	Install IPS	Thu 12 Nov '09	3 days	Mon 16 Nov '09	158	SP
160	NA	Install WAN Equipment	Tue 17 Nov '09	3 days	Thu 19 Nov '09	159	SP
161	NA	Installation Complete	Fri 20 Nov '09	3 days	Tue 24 Nov '09	160	SP
162	NA	Test connectivity	Wed 25 Nov '09	10 days	Tue 08 Dec '09	57,161	SP
163	NA	Suport SP with connectivity test	Wed 25 Nov '09	10 days	Tue 08 Dec '09	162SS	Prov
164	NA	Data Centre Network Complete	Tue 08 Dec '09	0 days	Tue 08 Dec '09	163	SP
165	NA	**Install STMS Interior Data Centre Networks (LAN & WAN) Project**	**Thu 04 Nov '10**	**135 days**	**Tue 10 May '11**		
166	NA	**Ordering**	**Thu 04 Nov '10**	**57 days**	**Thu 20 Jan '11**		
167	NA	Order circuits	Thu 04 Nov '10	0 days	Thu 04 Nov '10	25,142	Prov
168	NA	Order hardware	Thu 04 Nov '10	0 days	Thu 04 Nov '10	25,142	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
169	NA	Hardware received at an alternate SP location	Thu 20 Jan '11	0 days	Thu 20 Jan '11	168FS+57 days	SP
170	NA	**Configure Equipment (at an alternate SP location)**	**Fri 21 Jan '11**	**50 days**	**Thu 31 Mar '11**		
171	NA	Configure LAN core Switches	Fri 21 Jan '11	8 wks	Thu 17 Mar '11	169	SP
172	NA	Configure LAN TOR Switches	Fri 21 Jan '11	8 wks	Thu 17 Mar '11	171SS	SP
173	NA	Configure Firewalls	Fri 21 Jan '11	8 wks	Thu 17 Mar '11	171SS	SP
174	NA	Configure IPS	Fri 21 Jan '11	8 wks	Thu 17 Mar '11	171SS	SP
175	NA	Configure WAN	Fri 21 Jan '11	8 wks	Thu 17 Mar '11	171SS	SP
176	NA	Ship configured equipment to Interior DC	Fri 18 Mar '11	10 days	Thu 31 Mar '11	171,172,173,174,175	SP
177	NA	**Install Equipment (WAS Install & Configure)**	**Fri 01 Apr '11**	**18 days**	**Tue 26 Apr '11**		
178	NA	Install LAN core Switches	Fri 01 Apr '11	3 days	Tue 05 Apr '11	81,176	SP
179	NA	Install LAN TOR Switches	Wed 06 Apr '11	3 days	Fri 08 Apr '11	178	SP
180	NA	Install Firewalls	Mon 11 Apr '11	3 days	Wed 13 Apr '11	179	SP
181	NA	Install IPS	Thu 14 Apr '11	3 days	Mon 18 Apr '11	180	SP
182	NA	Install WAN Equipment	Tue 19 Apr '11	3 days	Thu 21 Apr '11	181	SP
183	NA	Installation Complete	Fri 22 Apr '11	3 days	Tue 26 Apr '11	182	SP
184	NA	Test connectivity	Wed 27 Apr '11	10 days	Tue 10 May '11	81,183	SP
185	NA	Suport SP with connectivity test	Wed 27 Apr '11	10 days	Tue 10 May '11	184SS	Prov
186	NA	Data Centre Network Complete	Tue 10 May '11	0 days	Tue 10 May '11	185	SP
187	NA	**Service Management Transformation**	**Mon 30 Mar '09**	**277 days?**	**Tue 13 Apr '10**		
188	NA	**Service Management Tool & Process Startup Project**	**Mon 30 Mar '09**	**134 days?**	**Sun 27 Sep '09**		
189	NA	**Service Mgmt Preparation Activities**	**Mon 30 Mar '09**	**10 days**	**Fri 10 Apr '09**		
190	NA	Confirm DW Implementation Date	Mon 30 Mar '09	1 day	Mon 30 Mar '09	5	SP
191	NA	Establishment of the Service Mgmt Team	Fri 10 Apr '09	0 days	Fri 10 Apr '09	5FS+10 days	SP
192	NA	**Implement SP Service Management Tool (DW)**	**Mon 06 Apr '09**	**121 days?**	**Tue 15 Sep '09**		
193	NA	**Build & testing of Digital Workflow**	**Mon 06 Apr '09**	**96 days?**	**Tue 11 Aug '09**		
194	Mon 06 Apr '09	DW Kickoff	Mon 06 Apr '09	4 days	Thu 09 Apr '09		SP
195	Tue 14 Apr '09	Data Gathering (collection & parsing incident management data)	Tue 14 Apr '09	45 days	Fri 12 Jun '09	194	SP
196	NA	Data Cut-off (DW templates are complete and approved and locked)	Fri 12 Jun '09	0 days	Fri 12 Jun '09	195	SP
197	NA	Client Approval (DW templates)	Fri 12 Jun '09	0 days	Fri 12 Jun '09	196	Prov
198	NA	Snapshot of ITIMS data loaded to DW Test Region	Mon 15 Jun '09	1 day?	Mon 15 Jun '09	197	SP
199	NA	Migrate snapshot data into DW test environment	Tue 16 Jun '09	31 days	Fri 24 Jul '09	198	SP
200	NA	Test Dispatch Interface from ITIMS to DW	Mon 13 Jul '09	10 days	Fri 24 Jul '09	199FF	SP
201	NA	Testing environment loaded	Fri 24 Jul '09	0 days	Fri 24 Jul '09	200	SP
202	NA	Final testing of DW and interface to ITIMS (without alarms)	Mon 27 Jul '09	5 days	Fri 31 Jul '09	201	SP
203	NA	Final testing of DW and interface to ITIMS (without alarms)	Mon 27 Jul '09	5 days	Fri 31 Jul '09	202FF	Prov
204	NA	Client concurrence on Production readiness	Fri 31 Jul '09	0 days	Fri 31 Jul '09	202FF	SP
205	NA	Reload with current production incident management data	Sat 01 Aug '09	7 days	Mon 10 Aug '09	204	SP
206	NA	Verify proper operation of Dispatch Interface from ITIMS to DW	Tue 11 Aug '09	1 day?	Tue 11 Aug '09	205	SP
207	NA	Data go live (Dispatch Interface is keeping DW synched with ITIMS)	Tue 11 Aug '09	0 days	Tue 11 Aug '09	206	SP
208	NA	**Addition of ITMS to DW (non-dispatch) interface & verification functions**	**Mon 15 Jun '09**	**70 days**	**Tue 15 Sep '09**		
209	NA	Design ITIMS to DW Interface (non-dispatch) plus verification functions	Mon 15 Jun '09	10 days	Wed 24 Jun '09	196	SP
210	NA	Develop & Test ITIMS to DW (non-dispatch) plus verification functions	Thu 25 Jun '09	50 days	Tue 01 Sep '09	209	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
211	NA	UAT testing of ITIMS to DW Interface (non-dispatch)	Wed 02 Sep '09	10 days	Tue 15 Sep '09	210	SP
212	NA	Support and Participation in UAT testing of ITMS to DW interface (non-dispatch)	Wed 02 Sep '09	10 days	Tue 15 Sep '09	211SS	Prov
213	NA	SP Service Management Tool (DW) is Production Ready	Tue 15 Sep '09	0 days	Tue 15 Sep '09	207,212	SP
214	NA	**Process Integration**	**Sat 18 Apr '09**	**114 days**	**Fri 18 Sep '09**		
215	Mon 27 Apr '09	Participate in Process Integration Workshop	Mon 27 Apr '09	5 days	Fri 01 May '09		SP
216	NA	Support SP and participate in Process Integration Workshop	Mon 27 Apr '09	5 days	Fri 01 May '09	215SS	Prov
217	NA	Operations Manual Outline - First Full Draft	Sat 18 Apr '09	34 days	Wed 03 Jun '09	5FS+15 days	SP
218	NA	Operations Manual First full draft	Thu 04 Jun '09	34 days	Fri 17 Jul '09	217	SP
219	NA	Operation Manual Complete	Mon 20 Jul '09	35 days	Thu 03 Sep '09	218	SP
220	NA	Future Mode of Operation (FMO) Training	Fri 04 Sep '09	11 days	Fri 18 Sep '09	219	SP
221	NA	SP Service Management Tool Training	Fri 18 Sep '09	1 day	Fri 18 Sep '09	220FF	SP
222	NA	**Asset Centre Module**	**Tue 16 Jun '09**	**61 days**	**Thu 03 Sep '09**		
223	NA	Initial Asset Centre Load	Tue 16 Jun '09	31 days	Fri 24 Jul '09	199FF	SP
224	NA	Final Asset inventory true-up	Wed 29 Jul '09	10 days	Mon 10 Aug '09	205FF	SP
225	NA	Support SP with the Final Asset inventory true-up	Wed 29 Jul '09	10 days	Mon 10 Aug '09	224SS	Prov
226	NA	Asset Module is Asset System of Record	Mon 10 Aug '09	0 days	Mon 10 Aug '09	225	SP
227	NA	Develop asset inventory reconciliation reporting	Mon 27 Jul '09	30 days	Thu 03 Sep '09	223	SP
228	NA	**SP Service Management Tool and Processes are Production Ready**	Fri 18 Sep '09	0 days	Fri 18 Sep '09	221,226,213	SP
229	NA	**Billing Module**	**Mon 27 Jul '09**	**42 days**	**Mon 21 Sep '09**		
230	NA	Configure and Test Volumetric Billing Inputs	Mon 27 Jul '09	32 days	Mon 07 Sep '09	223	SP
231	NA	Configure and Test Billing Function	Tue 11 Aug '09	30 days	Mon 21 Sep '09	224	SP
232	NA	Review and approve billing output	Tue 11 Aug '09	30 days	Mon 21 Sep '09	231SS	Prov
233	NA	Billing Module is ready for Production	Mon 21 Sep '09	0 days	Mon 21 Sep '09	232	SP
234	NA	**Reporting Portal**	**Mon 30 Mar '09**	**132 days**	**Wed 23 Sep '09**		
235	NA	Corporate eSLR instance in Canada ready to leverage	Mon 30 Mar '09	0 days	Mon 30 Mar '09	5	SP
236	NA	Develop Reporting Portal	Mon 30 Mar '09	66 days	Wed 24 Jun '09	235	SP
237	NA	Test and Refine Reports	Thu 25 Jun '09	66 days	Wed 23 Sep '09	236	SP
238	NA	Review and Approve Test Reports	Thu 25 Jun '09	66 days	Wed 23 Sep '09	237SS	Prov
239	NA	Reporting Portal Ready for Production	Wed 23 Sep '09	0 days	Wed 23 Sep '09	238	SP
240	Sun 27 Sep '09	**SP Service Management Tool and Process Go Live**	Sun 27 Sep '09	0 days	Sun 27 Sep '09		SP
241	NA	**Establish SLA Baseline (Month 7-12)**	**Thu 01 Oct '09**	**140 days**	**Tue 13 Apr '10**		
242	Thu 01 Oct '09	Six month Province mid-range server stability assessment (to be confirmed)	Wed 14 Oct '09	131 days	Tue 13 Apr '10	5SS+146 days,377	SP
243	Thu 01 Oct '09	Six month Province storage stability assessment (to be confirmed)	Thu 01 Oct '09	131 days	Wed 31 Mar '10	5SS+133 days,377,453	SP
244	NA	**Interface between iStore & DW for receiving requests (ALDEA) Project**	**Sun 01 Nov '09**	**1 day?**	**Sun 01 Nov '09**		
245	NA	project to be defined and dates to be determined	Sun 01 Nov '09	1 day?	Sun 01 Nov '09	228FS+30 days	SP
246	NA	**Mainframe Services Migration Project**	**Sun 01 Nov '09**	**437 days**	**Thu 30 Jun '11**		
247	NA	**Mainframe Migration Project**	**Sun 01 Nov '09**	**313 days**	**Fri 07 Jan '11**		
248	NA	**Mainframe Operational Assessment and Plan**	**Sun 01 Nov '09**	**66 days**	**Fri 29 Jan '10**		
249	Sun 01 Nov '09	Develop the Bridge Plan from SP to SP	Sun 01 Nov '09	66 days	Fri 29 Jan '10		S(
250	NA	Develop the Bridge Plan form SP to SP	Mon 07 Dec '09	40 days	Fri 29 Jan '10	249FF	Prov
251	NA	Schedule DR Test w/SunGuard	Fri 29 Jan '10	0 days	Fri 29 Jan '10	250	SP
252	NA	**Detailed Planning for migration of Mainframe Services**	**Mon 01 Feb '10**	**86 days**	**Mon 31 May '10**		

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
253	NA	Create the detailed plan for Mainframe Services Migration	Mon 01 Feb '10	86 days	Mon 31 May '10	249	SP
254	NA	Create the detailed plan for Mainframe Services Migration	Mon 01 Feb '10	86 days	Mon 31 May '10	250	Prov
255	NA	**Staff Preparation (plan to be confirmed and augmented by Detailed Planning)**	**Tue 01 Jun '10**	**151 days**	**Tue 28 Dec '10**		
256	NA	Training - vendor product	Tue 01 Jun '10	144 days	Fri 17 Dec '10	258SS	SP
257	NA	Training - operational	Tue 01 Jun '10	144 days	Fri 17 Dec '10	258SS	SP
258	NA	Documentation of current operational processes	Tue 01 Jun '10	144 days	Fri 17 Dec '10	282FF-12 days	SP
259	NA	Knowledge transfer of client requirements	Tue 01 Jun '10	144 days	Fri 17 Dec '10	258SS	SP
260	NA	Support knowledge transfer and documentation of current operational processes	Tue 01 Jun '10	144 days	Fri 17 Dec '10	258SS	Prov
261	NA	Update Authorization Matrices	Tue 28 Dec '10	1 day	Tue 28 Dec '10	282SS-5 days	Prov
262	NA	**Prepare Hardware Environment (plan to be confirmed and augmented by Detailed Plai**	**Tue 01 Jun '10**	**110 days**	**Mon 01 Nov '10**		
263	NA	Order mainframe, disk, tape, etc.	Tue 01 Jun '10	1 day	Tue 01 Jun '10	253	SP
264	Wed 13 Oct '10	Mainframe equipment received	Wed 13 Oct '10	1 day	Wed 13 Oct '10		SP
265	NA	Mainframe hardware installed in Calgary including Swing Gear	Thu 14 Oct '10	6 days	Thu 21 Oct '10	264	SP
266	NA	Mainframe hardware installed in DR site	Thu 14 Oct '10	13 days	Mon 01 Nov '10	264	SP
267	NA	**Prepare Software & Network Environments (plan to be confirmed and augmented by t**	**Mon 01 Feb '10**	**241 days**	**Sat 01 Jan '11**		
268	NA	Replace existing exits, usermods, utilities and automation that are not provided by incur	Mon 01 Feb '10	100 days	Fri 18 Jun '10	250	SP
269	NA	Load Mini-System on SP Calgary mainframe	Fri 22 Oct '10	11 days	Fri 05 Nov '10	265	SP
270	NA	Create IPL-able BUMP LPARs	Mon 08 Nov '10	6 days	Mon 15 Nov '10	269	SP
271	NA	Connect network between TELUS DASD to Calgary DASD	Fri 22 Oct '10	3 days	Tue 26 Oct '10	265	SP
272	NA	Support SP with connection network between TELUS DASD to Calgary DASD	Fri 22 Oct '10	3 days	Tue 26 Oct '10	271SS	Prov
273	NA	Initiate mirroring between TSDC DASD and Calgary DASD	Wed 27 Oct '10	6 days	Wed 03 Nov '10	272	SP
274	NA	Support SP with initiatation of mirroring between TSDC DASD and Calgary DASD	Wed 27 Oct '10	6 days	Wed 03 Nov '10	273SS	Prov
275	Thu 18 Nov '10	Mock 0 Migration	Thu 18 Nov '10	7 days	Fri 26 Nov '10	274,268	SP
276	NA	Mock 1 Migration	Mon 29 Nov '10	2 days	Tue 30 Nov '10	275	SP
277	NA	Support SP with Mock 1 Migration	Mon 29 Nov '10	2 days	Tue 30 Nov '10	276SS	Prov
278	NA	Mock 1 Sign-off by SP	Wed 01 Dec '10	1 day	Wed 01 Dec '10	277	SP
279	NA	Mock 1 Sign-off by Province	Wed 01 Dec '10	1 day	Wed 01 Dec '10	278SS	Prov
280	NA	Contingency period in case Mock 1 Migration neSP to be repeated	Wed 01 Dec '10	24 days	Sat 01 Jan '11	276	SP
281	NA	**Migration (plan to be confirmed and augmented by Detailed Planning)**	**Sun 02 Jan '11**	**6 days**	**Fri 07 Jan '11**		
282	Sun 02 Jan '11	Mock 2 Migration	Sun 02 Jan '11	1 day	Sun 02 Jan '11		SP
283	NA	Support SP with Mock 2 Migration	Sun 02 Jan '11	1 day	Sun 02 Jan '11	282SS	Prov
284	NA	Go Live/Mock 2 Sign-off by SP	Sun 02 Jan '11	0 days	Sun 02 Jan '11	283	SP
285	NA	Go Live/Mock 2 Sign-off by Province	Sun 02 Jan '11	0 days	Sun 02 Jan '11	284SS	Prov
286	NA	Initiate Mirroring betweeen Calgary DLm and DR Site DLm	Mon 03 Jan '11	5 days	Fri 07 Jan '11	282	SP
287	NA	Ship tapes from S15	Mon 03 Jan '11	5 days	Fri 07 Jan '11	285	SP
288	NA	Support SP with the shipment of tapes from S15	Mon 03 Jan '11	5 days	Fri 07 Jan '11	287SS	Prov
289	Tue 04 Jan '11	Disconnect network from TELUS	Tue 04 Jan '11	1 day	Tue 04 Jan '11	282	SP
290	NA	Support SP to disconnect network from TELUS	Tue 04 Jan '11	1 day	Tue 04 Jan '11	289SS	Prov
291	NA	**Mainframe Tape Transformation Project**	**Tue 04 Jan '11**	**128 days**	**Thu 30 Jun '11**		
292	Tue 04 Jan '11	Migrate data from tape media to VSM	Tue 04 Jan '11	128 days	Thu 30 Jun '11	282,265	SP
293	NA	Sign-off by SP on Migrated Data & Media Destruction	Thu 30 Jun '11	0 days	Thu 30 Jun '11	292	SP
294	NA	Sign-off by Province on Migrated Data & Media Destruction	Thu 30 Jun '11	0 days	Thu 30 Jun '11	293SS	Prov

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
295	NA	**Mainframe Disaster Recovery Test Project (date to be confirmed)**	**Mon 28 Feb '11**	**40 days**	**Fri 22 Apr '11**		
296	NA	DR Test	Mon 28 Feb '11	30 days	Fri 08 Apr '11	282FS+40 days,251	SP Oper
297	NA	Suport SP with DR Test	Mon 28 Feb '11	30 days	Fri 08 Apr '11	296SS	Prov
298	NA	DR Test Sign-off by SP	Mon 11 Apr '11	10 days	Fri 22 Apr '11	297	SP Oper
299	NA	DR Test Sign-off by Province	Mon 11 Apr '11	10 days	Fri 22 Apr '11	298SS	Prov
300	NA	**Server Systems Management Transformation**	**Fri 05 Sep '08**	**713 days**	**Thu 19 May '11**		
301	NA	**Assumption of Services Projects**	**Fri 05 Sep '08**	**261 days**	**Fri 28 Aug '09**		
302	NA	**Update Operating Documentation**	**Fri 05 Sep '08**	**125 days**	**Thu 26 Feb '09**		
303	NA	Create Server Systems Management Operating Manual (the "Manual")	Fri 05 Sep '08	125 days	Thu 26 Feb '09		SP
304	NA	**Perform Initial Anti Virus Scan for existing Government servers**	**Fri 24 Apr '09**	**59 days**	**Mon 13 Jul '09**		
305	NA	Ensure the Anti-Virus software is up to date (signature files and scan engines)	Fri 24 Apr '09	5 days	Thu 30 Apr '09	5FS+20 days	SP
306	NA	Schedule scans for all Province Servers (as applicable)	Thu 11 Jun '09	5 days	Wed 17 Jun '09	305,335	SP
307	NA	Schedule scans for Province Servers (as applicable)	Thu 11 Jun '09	5 days	Wed 17 Jun '09	306SS	Prov
308	NA	Execute scans on all Government server assets	Thu 18 Jun '09	20 days	Mon 13 Jul '09	307	SP
309	NA	**Perform Initial Security (Policy Compliance Management) scan on all servers**	**Mon 30 Mar '09**	**114 days**	**Fri 28 Aug '09**		
310	NA	Schedule scans for all Province Servers (as applicable)	Mon 30 Mar '09	30 days	Thu 07 May '09	5	SP
311	NA	Schedule scans for all Province Servers (as applicable)	Mon 30 Mar '09	30 days	Thu 07 May '09	310SS	Prov
312	NA	Scan Servers	Thu 11 Jun '09	30 days	Mon 20 Jul '09	311,336,102	SP
313	NA	Report Security PCM scan results to Province	Tue 21 Jul '09	30 days	Fri 28 Aug '09	312	SP
314	NA	**Add standard tools Projects**	**Tue 31 Mar '09**	**565 days**	**Thu 19 May '11**		
315	NA	**Set-up SP Tools for Province Data Centres**	**Tue 31 Mar '09**	**129 days**	**Mon 21 Sep '09**		
316	NA	Early order for Opsware HW/SW	Tue 31 Mar '09	1 day	Tue 31 Mar '09	24	SP
317	NA	Order balance of HW and SW	Fri 03 Apr '09	5 days	Thu 09 Apr '09	25	SP
318	NA	CA & Opsware HW/SW delivered	Mon 27 Apr '09	0 days	Mon 27 Apr '09	316FS+20 days	SP
319	NA	Balance of HW/SW order delivered	Wed 06 May '09	0 days	Wed 06 May '09	317FS+20 days	SP
320	NA	**Set-up SP software distribution infrastructure for Opsware**	**Fri 10 Apr '09**	**25 days**	**Wed 13 May '09**		
321	NA	Schedule time with Facility and network personnel	Fri 10 Apr '09	2 days	Mon 13 Apr '09	317	SP
322	NA	Open Change Management Records	Tue 14 Apr '09	1 day	Tue 14 Apr '09	321	SP
323	NA	Rack and Stack Opsware Satellite Servers	Tue 28 Apr '09	10 days	Mon 11 May '09	318	SP
324	NA	Build Opsware Satellite Servers	Tue 12 May '09	2 days	Wed 13 May '09	323	SP
325	NA	Opsware infrastructure setup is complete	Wed 13 May '09	0 days	Wed 13 May '09	324	SP
326	NA	**Set-up SP monitoring infrastructure for CA**	**Fri 10 Apr '09**	**30 days**	**Wed 20 May '09**		
327	NA	Schedule time with Facility and network personnel	Fri 10 Apr '09	2 days	Mon 13 Apr '09	317	SP
328	NA	Open Change Management Records	Tue 14 Apr '09	1 day	Tue 14 Apr '09	327	SP
329	NA	Rack and stack Computer Associates (CA) Infrastructure Servers	Tue 28 Apr '09	10 days	Mon 11 May '09	318	SP
330	NA	Connect to SP Canada Network	Tue 12 May '09	5 days	Mon 18 May '09	**329,102**	SP
331	NA	SP Canada Tools Team to build CA infrastructure servers	Tue 19 May '09	2 days	Wed 20 May '09	330	SP
332	NA	CA infrastructure setup is complete	Wed 20 May '09	0 days	Wed 20 May '09	331	SP
333	NA	Province Data Centre - Build Server Administration Servers	Thu 07 May '09	10 days	Wed 20 May '09	5,319	SP
334	NA	Province Data Centre - Build backup & storage toolset S. 15	Thu 07 May '09	10 days	Wed 20 May '09	5,319	SP
335	NA	Province Data Centre - Set-up SP Anti Virus Infrastructure	Thu 14 May '09	20 days	Wed 10 Jun '09	5,325,319	SP
336	NA	Province Data Centre - Set-up SP PCM (Policy Compliance Management) Hardware	Thu 14 May '09	20 days	Wed 10 Jun '09	5,325,319	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
337	NA	**Rollout SP Tool Agents to all Mid-Range servers**	**Fri 17 Apr '09**	**116 days**	**Mon 21 Sep '09**		
338	NA	**Conduct Opsware Agent Rollout Test**	**Fri 17 Apr '09**	**50 days**	**Mon 22 Jun '09**		
339	NA	Determine and document Opsware agent install activities/processes	Thu 23 Apr '09	15 days	Wed 13 May '09	325FF	SP
340	NA	Prepare the lab systems as typical clients	Thu 14 May '09	10 days	Wed 27 May '09	**339,102,319**	SP
341	NA	Coordinate with all stakeholders	Fri 17 Apr '09	30 days	Wed 27 May '09	340FF	SP
342	NA	Support SP to coordinate with all stakeholders	Fri 17 Apr '09	30 days	Wed 27 May '09	341SS	Prov
343	NA	Perform Tests	Thu 28 May '09	10 days	Wed 10 Jun '09	342,325	SP
344	NA	Analyze the results	Thu 11 Jun '09	5 days	Wed 17 Jun '09	343	SP
345	NA	Support SP with Analyzing Results	Thu 11 Jun '09	5 days	Wed 17 Jun '09	344SS	Prov
346	NA	Test Results accepted by SP	Thu 18 Jun '09	5 days	Mon 22 Jun '09	345	SP
347	NA	Test Results accepted by Province	Thu 18 Jun '09	5 days	Mon 22 Jun '09	346SS	Prov
348	NA	**Conduct CA Agent Rollout Test**	**Thu 23 Apr '09**	**50 days**	**Mon 29 Jun '09**		
349	NA	Determine and document CA agent install activities/processes	Thu 30 Apr '09	15 days	Wed 20 May '09	332FF	SP
350	NA	Prepare the lab systems as typical client servers	Thu 21 May '09	10 days	Wed 03 Jun '09	**102,349,319**	SP
351	NA	Coordinate with all Stakeholders	Thu 23 Apr '09	30 days	Wed 03 Jun '09	350FF	SP
352	NA	Support SP with the coordination of Stakeholders	Thu 23 Apr '09	30 days	Wed 03 Jun '09	351SS	Prov
353	NA	Perform Tests	Thu 04 Jun '09	10 days	Wed 17 Jun '09	352,332	SP
354	NA	Analyze the results	Thu 18 Jun '09	5 days	Mon 22 Jun '09	353	SP
355	NA	Support SP with analyzing CA Agent Rollout Test Results	Thu 18 Jun '09	5 days	Mon 22 Jun '09	354SS	Prov
356	NA	Test Results accepted by SP	Tue 23 Jun '09	5 days	Mon 29 Jun '09	355	SP
357	NA	Test Results accepted by Province	Tue 23 Jun '09	5 days	Mon 29 Jun '09	356SS	Prov
358	NA	**Conduct** S. 15 **Rollout Pilot**	**Thu 11 Jun '09**	**21 days**	**Tue 07 Jul '09**		
359	NA	Identify Pilot group for testing automatic agent deployment	Thu 11 Jun '09	10 days	Mon 22 Jun '09	338FF	SP
360	NA	Support SP to Identify Pilot group for testing agent deployment	Thu 11 Jun '09	10 days	Mon 22 Jun '09	359SS	Prov
361	NA	Schedule the pilot	Tue 23 Jun '09	5 days	Mon 29 Jun '09	360	SP
362	NA	Pilot S. 15 deployment process	Tue 30 Jun '09	5 days	Mon 06 Jul '09	361	SP
363	NA	Analyze the results	Tue 07 Jul '09	1 day	Tue 07 Jul '09	362	SP
364	NA	Support SP to Analyze results	Tue 07 Jul '09	1 day	Tue 07 Jul '09	363SS	Prov
365	NA	Approval to use S. 15 technology for production rollou	Tue 07 Jul '09	0 days	Tue 07 Jul '09	364	Prov
366	NA	S. 15 **Rollout Pilot**	**Thu 18 Jun '09**	**21 days**	**Tue 14 Jul '09**		
367	NA	Identify Pilot group for testing agent deployment	Thu 18 Jun '09	10 days	Mon 29 Jun '09	348FF	SP
368	NA	Support SP with identifying Pilot group for testing agent deployment	Thu 18 Jun '09	10 days	Mon 29 Jun '09	367SS	Prov
369	NA	Schedule the pilot	Tue 30 Jun '09	5 days	Mon 06 Jul '09	368	SP
370	NA	Pilot S. 15 deployment processes	Tue 07 Jul '09	5 days	Mon 13 Jul '09	369	SP
371	NA	Analyze the results	Tue 14 Jul '09	1 day	Tue 14 Jul '09	370	SP
372	NA	Support SP with Analyzing Results	Tue 14 Jul '09	1 day	Tue 14 Jul '09	371SS	Prov
373	NA	**Conduct** S. 15 **Rollout to Production**	**Wed 08 Jul '09**	**15 days**	**Tue 28 Jul '09**		
374	NA	Automated deployment of SP monitoring agents for S. 15	Wed 08 Jul '09	15 days	Tue 28 Jul '09	358	SP
375	NA	Support SP with automated deployment of SP monitoring agents for S. 15	Wed 08 Jul '09	15 days	Tue 28 Jul '09	374SS	Prov
376	NA	**Conduct** S. 15 **Rollout to Production**	**Wed 15 Jul '09**	**50 days**	**Mon 21 Sep '09**		
377	NA	Install SP monitoring agents fo S. 15	Wed 15 Jul '09	50 days	Mon 21 Sep '09	**126,366**	SP
378	NA	Support SP with install of montoring agents fo S. 15	Wed 15 Jul '09	50 days	Mon 21 Sep '09	377SS	Prov

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
379	NA	Remove existing Province monitoring agents as necessary	Wed 15 Jul '09	50 days	Mon 21 Sep '09	326,320,377SS,374SS	SP
380	NA	Support SP with the removal of existing Province Agents as necessary	Wed 15 Jul '09	50 days	Mon 21 Sep '09	379SS	Prov
381	NA	**Set-up SP Tools for STMS Calgary Data Centre**	**Mon 07 Sep '09**	**75 days**	**Thu 17 Dec '09**		
382	NA	Obtain approval to procure hardware/software (CAN)	Mon 07 Sep '09	4 days	Thu 10 Sep '09	57SS-40 days	SP
383	NA	Order HW/SW	Mon 14 Sep '09	5 days	Fri 18 Sep '09	57SS-35 days	SP
384	NA	HW/SW Delivered	Sun 01 Nov '09	1 day	Sun 01 Nov '09	57SS	SP
385	NA	**Set-up Opsware Infra - STMS Calgary**	**Sun 01 Nov '09**	**15 days**	**Thu 19 Nov '09**		
386	NA	Schedule time with Facility and network personnel	Sun 01 Nov '09	2 days	Mon 02 Nov '09	57	SP
387	NA	Open Change Management Records	Tue 03 Nov '09	1 day	Tue 03 Nov '09	386	SP
388	NA	Deploy Opsware Satellite Servers	Wed 04 Nov '09	10 days	Tue 17 Nov '09	387	SP
389	NA	Build Opsware Servers	Wed 18 Nov '09	2 days	Thu 19 Nov '09	388	SP
390	NA	Opsware infrastructure setup is complete	Thu 19 Nov '09	0 days	Thu 19 Nov '09	389	SP
391	NA	**Set-up CA monitoring infra - STMS Calgary**	**Sun 01 Nov '09**	**35 days**	**Thu 17 Dec '09**		
392	NA	Schedule time with Facility and network personnel	Sun 01 Nov '09	2 days	Mon 02 Nov '09	57	SP
393	NA	Open Change Management Records	Tue 03 Nov '09	1 day	Tue 03 Nov '09	392	SP
394	NA	Deploy Computer Associates S. 15	Wed 04 Nov '09	10 days	Tue 17 Nov '09	393	SP
395	NA	Connect to SP Canada Network	Wed 09 Dec '09	5 days	Tue 15 Dec '09	394,162	SP
396	NA	SP Canada Tools Team to build CA infrastructure servers	Wed 16 Dec '09	2 days	Thu 17 Dec '09	395	SP
397	NA	CA infrastructure setup is complete	Thu 17 Dec '09	0 days	Thu 17 Dec '09	396	SP
398	NA	STMS Calgary - Set-up SP Anti Virus Infrastructure	Fri 20 Nov '09	20 days	Thu 17 Dec '09	390,57	SP
399	NA	STMS Calgary - Set-up Event Log Collection toolset	Fri 20 Nov '09	20 days	Thu 17 Dec '09	390,57	SP
400	NA	STMS Calgary - Build Network toolset S. 15	Fri 04 Dec '09	10 days	Thu 17 Dec '09	57FS+25 days	SP
401	NA	STMS Calgary - Build storage & backup toolset S. 15	Fri 04 Dec '09	10 days	Thu 17 Dec '09	57FS+25 days	SP
402	NA	**Set-up SP Tools for STMS Interior**	**Fri 04 Feb '11**	**75 days**	**Thu 19 May '11**		
403	NA	Obtain approval to procure hardware/software (CAN)	Fri 04 Feb '11	4 days	Wed 09 Feb '11	81SS-40 days	SP
404	NA	Order HW/SW	Fri 11 Feb '11	5 days	Thu 17 Feb '11	81SS-35 days	SP
405	NA	HW/SW Delivered	Fri 01 Apr '11	1 day	Fri 01 Apr '11	81SS	SP
406	NA	**Set-up** S. 15 **- STMS Interior**	**Fri 01 Apr '11**	**15 days**	**Thu 21 Apr '11**		
407	NA	Schedule time with Facility and network personnel	Fri 01 Apr '11	2 days	Mon 04 Apr '11	81	SP
408	NA	Open Change Management Records	Tue 05 Apr '11	1 day	Tue 05 Apr '11	407	SP
409	NA	Deploy S. 15	Wed 06 Apr '11	10 days	Tue 19 Apr '11	408	SP
410	NA	Build S. 15 Servers	Wed 20 Apr '11	2 days	Thu 21 Apr '11	409	SP
411	NA	Opsware infrastructure setup is complete	Thu 21 Apr '11	0 days	Thu 21 Apr '11	410	SP
412	NA	**Set-up** S. 15 **- STMS Interior**	**Fri 01 Apr '11**	**35 days**	**Thu 19 May '11**		
413	NA	Schedule time with Facility and network personnel	Fri 01 Apr '11	2 days	Mon 04 Apr '11	81	SP
414	NA	Open Change Management Records	Tue 05 Apr '11	1 day	Tue 05 Apr '11	413	SP
415	NA	Deploy Computer Associates S. 15	Wed 06 Apr '11	10 days	Tue 19 Apr '11	414	SP
416	NA	Connect to SP Canada Network	Wed 11 May '11	5 days	Tue 17 May '11	415,184	SP
417	NA	SP Canada Tools Team to build CA infrastructure servers	Wed 18 May '11	2 days	Thu 19 May '11	416	SP
418	NA	CA infrastructure setup is complete	Thu 19 May '11	0 days	Thu 19 May '11	417	SP
419	NA	STMS Interior - Set-up SP Anti Virus Infrastructure	Fri 22 Apr '11	20 days	Thu 19 May '11	411,81	SP
420	NA	STMS Interior - Set up Event log collection toolset	Fri 22 Apr '11	20 days	Thu 19 May '11	411,81	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
421	NA	STMS Interior - Build Network toolset	Fri 06 May '11	10 days	Thu 19 May '11	81FS+25 days	SP
422	NA	STMS Interior - Build storage toolset	Fri 06 May '11	10 days	Thu 19 May '11	81FS+25 days	SP
423	NA	**Shared File and Print Redesign Project**	**Tue 06 Oct '09**	**340 days**	**Wed 19 Jan '11**		
424	NA	Project Plan not yet developed (timing to be confirmed)	Tue 06 Oct '09	17 mons	Wed 19 Jan '11	5SS+7 mons	SP
425	NA	**Virtulization Assesment and Migration Planning Project**	**Mon 30 Mar '09**	**100 days**	**Mon 10 Aug '09**		
426	NA	**Establish Server Test Lab for Refresh**	**Thu 07 May '09**	**24 days**	**Tue 09 Jun '09**	**319**	
427	NA	Establish lab space in Victoria BC	Tue 02 Jun '09	5 days	Mon 08 Jun '09	44	SP
428	NA	Order Hardware	Thu 07 May '09	1 day	Thu 07 May '09	44FS-30 days	SP
429	NA	Receive Hardware	Mon 01 Jun '09	1 day	Mon 01 Jun '09	44FF	SP
430	NA	Build SP Standard Server Environment	Tue 02 Jun '09	5 days	Mon 08 Jun '09	429	SP
431	NA	Confirm lab build to meet project requirements Sign-off	Tue 09 Jun '09	1 day	Tue 09 Jun '09	430	SP
432	NA	**Establish Virtualization Assement and Migration plans**	**Mon 30 Mar '09**	**100 days**	**Mon 10 Aug '09**		
433	NA	Virtualization Assement and Migration Planning Start-Up	Mon 30 Mar '09	1 mon	Thu 23 Apr '09	5	SP
434	NA	**Virtualization Assement and Migration Study**	**Fri 24 Apr '09**	**40 days**	**Thu 18 Jun '09**		**SP**
435	NA	Deliverable: Reference Architecture	Fri 24 Apr '09	2 mons	Thu 18 Jun '09	433	SP
436	NA	Deliverable: Recommended Source to Target Report	Fri 24 Apr '09	2 mons	Thu 18 Jun '09	433	SP
437	NA	**Virtualization and Migration Multi-Year Plan Development**	**Fri 19 Jun '09**	**40 days**	**Mon 10 Aug '09**		**SP**
438	NA	Deliverable: Multi-Year Virtualization and Migration Plan	Fri 19 Jun '09	2 mons	Mon 10 Aug '09	434	SP
439	NA	Deliverable: Identification of Apps & Data that must migrate with Mainframe services	Fri 19 Jun '09	2 mons	Mon 10 Aug '09	434	SP
440	NA	Deliverable: Concurrence on first Committed Annual Plan (2 Migration Waves)	Fri 19 Jun '09	2 mons	Mon 10 Aug '09	434	SP
441	NA	**Virtualization and Migration Multi-Year Plan Development**	**Fri 19 Jun '09**	**40 days**	**Mon 10 Aug '09**		**Prov**
442	NA	Deliverable: Concurrence on Multi-Year Virtualization and Migration Plan	Fri 19 Jun '09	2 mons	Mon 10 Aug '09	438SS	Prov
443	NA	Deliverable: Concurrence on Apps & Data that must migrate with Mainframe services	Fri 19 Jun '09	2 mons	Mon 10 Aug '09	439SS	Prov
444	NA	Deliverable: Concurrence on first Committed Annual Plan (2 Migration Waves)	Fri 19 Jun '09	2 mons	Mon 10 Aug '09	440SS	Prov
445	NA	**Field Services Transformation**	**Mon 30 Mar '09**	**1 day**	**Mon 30 Mar '09**		
446	NA	Provide SP with warranty information for existing BC Government servers	Mon 30 Mar '09	1 day	Mon 30 Mar '09	5	Prov
447	NA	Assume responsibility for provision of maintance and other related Field Services	Mon 30 Mar '09	1 day	Mon 30 Mar '09	5	SP
448	NA	**Storage Management & Back-up Management Transformation**	**Mon 30 Mar '09**	**587 days**	**Fri 17 Jun '11**		
449	NA	**Install Service Provider Toolkit on Province Infrastructure**	**Mon 30 Mar '09**	**110 days**	**Mon 24 Aug '09**		
450	NA	Tools Training (i.e. ECC, Reporting, etc.)	Mon 30 Mar '09	56 days	Fri 12 Jun '09	5	SP
451	NA	Add SP Standard tools	Fri 24 Apr '09	90 days	Mon 24 Aug '09	452FF	SP
452	NA	Remove existing tools as required	Tue 14 Jul '09	31 days	Mon 24 Aug '09	126	SP
453	NA	SP Backup and Storage Processes fully implemented	Mon 24 Aug '09	0 days	Mon 24 Aug '09	452FF	SP
454	NA	Develop Managed Storage and Managed Backup Operating Manual	Mon 30 Mar '09	110 days	Mon 24 Aug '09	5	SP
455	NA	**STMS Data Centres**	**Mon 21 Sep '09**	**458 days**	**Fri 17 Jun '11**		
456	NA	**STMS Data Centre - Calgary Storage & Backup Install Project**	**Mon 21 Sep '09**	**76 days**	**Fri 01 Jan '10**		
457	NA	HW/SW ordered	Mon 21 Sep '09	1 day	Mon 21 Sep '09	57FS-30 days	SP
458	NA	Update Operating Manual for Calgary	Fri 02 Oct '09	1 mon	Fri 30 Oct '09	459SF-1 day	SP
459	NA	HW/SW Delivered	Sun 01 Nov '09	1 day	Sun 01 Nov '09	457FS+22 days,57	SP
460	NA	Install SSMS monitoring & management environment	Fri 18 Dec '09	11 days	Fri 01 Jan '10	155,401,57	SP
461	NA	Install new SAN switches	Mon 02 Nov '09	21 days	Mon 30 Nov '09	459	SP
462	NA	Install new Storage Arrays	Tue 01 Dec '09	10 days	Mon 14 Dec '09	461	SP

S. 15

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
463	NA	Install new backup EDL's	Mon 02 Nov '09	1 day	Mon 02 Nov '09	459	SP
464	NA	Install new backup master & media servers	Mon 02 Nov '09	1 day	Mon 02 Nov '09	459	SP
465	NA	Install new backup tape library	Mon 02 Nov '09	1 day	Mon 02 Nov '09	459	SP
466	NA	Configure backup jobs	Wed 09 Dec '09	2 days	Thu 10 Dec '09	162,463,464	SP
467	NA	Test EDL & Tape Library, SAN Switches, SAN Storage Arrays	Fri 11 Dec '09	5 days	Thu 17 Dec '09	162,463,464,465,466	SP
468	NA	Test Site to Site Replication	Fri 18 Dec '09	3 days	Tue 22 Dec '09	467	SP
469	NA	Sign-off by SP that Infrastructure is ready to receive data	Wed 23 Dec '09	1 day	Wed 23 Dec '09	468,467	SP
470	NA	Sign-off by Province that Infrastructure is ready to receive data	Wed 23 Dec '09	1 day	Wed 23 Dec '09	469SS	Prov
471	NA	Contingency time	Thu 24 Dec '09	6 days	Thu 31 Dec '09	470	SP
472	NA	**STMS Data Centre - Interior Storage & Backup Install Project**	**Fri 18 Feb '11**	**86 days**	**Fri 17 Jun '11**		
473	NA	HW/SW ordered	Fri 18 Feb '11	1 day	Fri 18 Feb '11	81FS-30 days	SP
474	NA	Update Operating Manual for Interior	Thu 03 Mar '11	1 mon	Thu 31 Mar '11	475SF-1 day	SP
475	NA	HW/SW Delivered	Fri 01 Apr '11	1 day	Fri 01 Apr '11	473FS+23 days,81	SP
476	NA	Install SSMS monitoring & management environment	Fri 20 May '11	10 days	Thu 02 Jun '11	422,177,81	SP
477	NA	Install new SAN switches	Mon 04 Apr '11	11 days	Mon 18 Apr '11	475	SP
478	NA	Install new Storage Arrays	Fri 03 Jun '11	11 days	Fri 17 Jun '11	476	SP
479	NA	Install new backup EDL's	Mon 04 Apr '11	1 day	Mon 04 Apr '11	475	SP
480	NA	Install new backup master & media servers	Mon 04 Apr '11	1 day	Mon 04 Apr '11	475	SP
481	NA	Install new backup Tape Library	Mon 04 Apr '11	1 day	Mon 04 Apr '11	475	SP
482	NA	Configure backup jobs	Wed 11 May '11	2 days	Thu 12 May '11	479,480,184	SP
483	NA	Test EDL & Tape Library, SAN Switches & SAN Storage Arrays	Wed 11 May '11	5 days	Tue 17 May '11	479,480,481,184	SP
484	NA	Test Site to Site Replication	Wed 18 May '11	3 days	Fri 20 May '11	483	SP
485	NA	Sign-off by SP that Infrastructure is ready to receive data	Mon 23 May '11	1 day	Mon 23 May '11	484	SP
486	NA	Sign-off by Province that Infrastructure is ready to receive data	Mon 23 May '11	1 day	Mon 23 May '11	485SS	Prov
487	NA	Contingency time	Tue 24 May '11	6 days	Tue 31 May '11	486	SP
488	NA	**After Hours Service Desk Transformation (Optional Project)**	**Mon 30 Mar '09**	**81 days**	**Wed 15 Jul '09**		
489	NA	P.I.A. (Process Integration Activities)	Mon 30 Mar '09	65 days	Tue 23 Jun '09	5	SP
490	NA	Support SP with P.I.A (Process Integration Activities)	Mon 30 Mar '09	65 days	Tue 23 Jun '09	489SS	Prov
491	NA	EKMS Implementation	Mon 13 Apr '09	10 days	Thu 23 Apr '09	5FS+10 days	SP
492	Fri 01 May '09	Agent training complete	Fri 01 May '09	43 days	Fri 26 Jun '09		SP
493	Mon 01 Jun '09	ACD Implemented	Mon 01 Jun '09	22 days	Fri 26 Jun '09		SP
494	Mon 01 Jun '09	Customer Acceptance	Mon 01 Jun '09	22 days	Fri 26 Jun '09		SP
495	Wed 15 Jul '09	After Hours Service Desk Go Live (date to be confirmed)	Wed 15 Jul '09	1 day	Wed 15 Jul '09	494	SP
496	NA	**Security Transfomation**	**Mon 30 Mar '09**	**754 days**	**Tue 07 Feb '12**		
497	NA	**Privileged Access ID Management Improvement Project (dates to be confirmed)**	**Mon 30 Mar '09**	**754 days**	**Tue 07 Feb '12**		
498	NA	Review Province privileged ID Management policy & procedures	Mon 30 Mar '09	231 days	Mon 08 Feb '10	5	SP
499	NA	Review Province privileged ID Management policy & procedures	Mon 30 Mar '09	231 days	Mon 08 Feb '10	5	Prov
500	NA	Develop a plan to improve privileged ID Management	Tue 09 Feb '10	261 days	Fri 04 Feb '11	499	SP
501	NA	Develop a plan to improve privileged ID Management	Tue 09 Feb '10	261 days	Fri 04 Feb '11	500SS	Prov
502	NA	Implement agreed/approved elements of the improvement plan	Mon 07 Feb '11	262 days	Tue 07 Feb '12	500,501	SP
503	NA	Implement agreed/approved elements of the improvement plan	Mon 07 Feb '11	262 days	Tue 07 Feb '12	502SS	Prov
504	NA	**Optional Security Services Projects (no dates are committed)**	**Thu 31 Dec '09**	**0 days**	**Thu 31 Dec '09**		

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
505	Thu 31 Dec '09	Security Information Management / Enterprise Security Event Project (to be confirmed by Pr	Thu 31 Dec '09	0 days	Thu 31 Dec '09		SP
506	Thu 31 Dec '09	Payment Card Industry Data Security Standard Compliant Infrastructure Project (to be confir	Thu 31 Dec '09	0 days	Thu 31 Dec '09		SP
507	Thu 31 Dec '09	"Two Factors Authentication Project for Service Provider Privileged Access (to be confirmed	Thu 31 Dec '09	0 days	Thu 31 Dec '09		SP
508	Thu 31 Dec '09	"Two Factors Authentication Project for Province Privileged Access (to be confirmed by Prov	Thu 31 Dec '09	0 days	Thu 31 Dec '09		SP
509	NA	**Virtualization & Migration Project**	**Tue 11 Aug '09**	**1213 days**	**Mon 31 Mar '14**		
510	NA	**Committed Annual Plan1 - 10% servers**	**Tue 11 Aug '09**	**168 days**	**Wed 31 Mar '10**		
511	NA	**Committed Annual Plan1 Wave 1 (Pilot Wave)**	**Tue 11 Aug '09**	**104 days**	**Thu 31 Dec '09**		
512	NA	Order HW/SW for wave	Tue 11 Aug '09	1 day	Tue 11 Aug '09	444	SP
513	NA	Develop Detailed Plan for migration wave	Wed 12 Aug '09	1 mon	Tue 08 Sep '09	512	SP
514	NA	Approve Detailed Plan for migration wave	Tue 08 Sep '09	0 days	Tue 08 Sep '09	513	Prov
515	NA	Install and configure HW/SW before migration wave	Wed 09 Sep '09	1 mon	Tue 06 Oct '09	512FS+1 mon	SP
516	NA	Execute migration plan to Province DCs	Wed 07 Oct '09	63 days	Thu 31 Dec '09	514,515	SP
517	NA	**Committed Annual Plan1 Wave 2**	**Mon 12 Oct '09**	**124 days**	**Wed 31 Mar '10**		
518	NA	Client consultation to re-confirm wave content	Mon 12 Oct '09	1 mon	Thu 05 Nov '09	524SS-3 mons	SP
519	NA	Re-confirm wave content	Thu 05 Nov '09	0 days	Thu 05 Nov '09	518	Prov
520	NA	Order HW/SW for wave	Fri 06 Nov '09	1 day	Fri 06 Nov '09	519	SP
521	NA	Develop Detailed Plan for migration wave	Fri 06 Nov '09	1 mon	Thu 03 Dec '09	524SS-2 mons	SP
522	NA	Approve Detailed Plan for migration wave	Thu 03 Dec '09	0 days	Thu 03 Dec '09	521	Prov
523	NA	Install and configure HW/SW before migration wave	Mon 07 Dec '09	1 mon	Fri 01 Jan '10	520FS+1 mon	SP
524	NA	Execute migration plan to Calgary or Province DCs	Fri 01 Jan '10	64 days	Wed 31 Mar '10	516	SP
525	NA	**Committed Annual Plan 2 - 20% of servers**	**Tue 01 Dec '09**	**350 days**	**Thu 31 Mar '11**		
526	Tue 01 Dec '09	Refine and Approve Second Committed Annual Plan of the Multi-Year Plan	Tue 01 Dec '09	2 mons	Mon 25 Jan '10		SP
527	NA	**Refine and Approve Second Committed Annual Plan of the Multi-Year Plan**	**Tue 01 Dec '09**	**2 mons**	**Mon 25 Jan '10**	**526SS**	**Prov**
528	NA	**Committed Annual Plan 2 Wave 1**	**Tue 26 Jan '10**	**112 days**	**Wed 30 Jun '10**		
529	NA	Order HW/SW for wave	Tue 26 Jan '10	1 day	Tue 26 Jan '10	527	SP
530	NA	Develop Detailed Plan for migration wave	Tue 26 Jan '10	1 mon	Mon 22 Feb '10	527	SP
531	NA	Approve Detailed Plan for migration wave	Mon 22 Feb '10	0 days	Mon 22 Feb '10	530	Prov
532	NA	Install and configure HW/SW before migration wave	Wed 24 Feb '10	1 mon	Tue 23 Mar '10	529FS+1 mon	SP
533	NA	Execute migration plan to Calgary or Province DCs	Thu 01 Apr '10	65 days	Wed 30 Jun '10	524	SP
534	NA	**Committed Annual Plan 2 Wave 2**	**Thu 08 Apr '10**	**126 days**	**Thu 30 Sep '10**		
535	NA	Client consultation to re-confirm wave content	Thu 08 Apr '10	1 mon	Wed 05 May '10	541SS-3 mons	SP
536	NA	Re-confirm wave content	Wed 05 May '10	0 days	Wed 05 May '10	535	Prov
537	NA	Order HW/SW for wave	Thu 06 May '10	1 day	Thu 06 May '10	536	SP
538	NA	Develop Detailed Plan for migration wave	Thu 06 May '10	1 mon	Wed 02 Jun '10	541SS-2 mons	SP
539	NA	Approve Detailed Plan for migration wave	Wed 02 Jun '10	0 days	Wed 02 Jun '10	538	Prov
540	NA	Install and configure HW/SW before migration wave	Fri 04 Jun '10	1 mon	Thu 01 Jul '10	537FS+1 mon	SP
541	NA	Execute migration plan to Calgary or Province DCs	Thu 01 Jul '10	66 days	Thu 30 Sep '10	533	SP
542	NA	**Committed Annual Plan 2 Wave 3**	**Fri 09 Jul '10**	**126 days**	**Fri 31 Dec '10**		
543	NA	Client consultation to re-confirm wave content	Fri 09 Jul '10	1 mon	Thu 05 Aug '10	549SS-3 mons	SP
544	NA	Re-confirm wave content	Thu 05 Aug '10	0 days	Thu 05 Aug '10	543	Prov
545	NA	Order HW/SW for wave	Fri 06 Aug '10	1 day	Fri 06 Aug '10	544	SP
546	NA	Develop Detailed Plan for migration wave	Fri 06 Aug '10	1 mon	Thu 02 Sep '10	549SS-2 mons	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
547	NA	Approve Detailed Plan for migration wave	Thu 02 Sep '10	0 days	Thu 02 Sep '10	546	Prov
548	NA	Install and configure HW/SW before migration wave	Mon 06 Sep '10	1 mon	Fri 01 Oct '10	545FS+1 mon	SP
549	NA	Execute migration plan to Calgary or Province DCs	Fri 01 Oct '10	66 days	Fri 31 Dec '10	541	SP
550	NA	**Mainframe migration wave**	**Wed 14 Jul '10**	**125 days**	**Sun 02 Jan '11**		
551	NA	Client consultation to re-confirm wave content	Wed 14 Jul '10	1 mon	Tue 10 Aug '10	557SS-3 mons	SP
552	NA	Re-confirm wave content	Tue 10 Aug '10	0 days	Tue 10 Aug '10	551	Prov
553	NA	Order HW/SW for wave	Wed 11 Aug '10	1 day	Wed 11 Aug '10	552	SP
554	NA	Develop Detailed Plan for migration wave	Wed 11 Aug '10	1 mon	Tue 07 Sep '10	557SS-2 mons	SP
555	NA	Approve Detailed Plan for migration wave	Tue 07 Sep '10	0 days	Tue 07 Sep '10	554	Prov
556	NA	Install and configure HW/SW before migration wave	Thu 09 Sep '10	1 mon	Wed 06 Oct '10	553FS+1 mon	SP
557	NA	Execute migration plan to Calgary DC (for Mid-Range servers that must migrate with th	Wed 06 Oct '10	65 days	Sun 02 Jan '11	282FF	SP
558	NA	**Committed Annual Plan 2 Wave 4**	**Mon 11 Oct '10**	**126 days**	**Thu 31 Mar '11**		
559	NA	Client consultation to re-confirm wave content	Mon 11 Oct '10	1 mon	Fri 05 Nov '10	565SS-3 mons	SP
560	NA	Re-confirm wave content	Fri 05 Nov '10	0 days	Fri 05 Nov '10	559	Prov
561	NA	Order HW/SW for wave	Mon 08 Nov '10	1 day	Mon 08 Nov '10	560	SP
562	NA	Develop Detailed Plan for migration wave	Mon 08 Nov '10	1 mon	Fri 03 Dec '10	565SS-2 mons	SP
563	NA	Approve Detailed Plan for migration wave	Fri 03 Dec '10	0 days	Fri 03 Dec '10	562	Prov
564	NA	Install and configure HW/SW before migration wave	Tue 07 Dec '10	1 mon	Sat 01 Jan '11	561FS+1 mon	SP
565	NA	Execute migration plan to Calgary or Province DCs	Sat 01 Jan '11	66 days	Thu 31 Mar '11	549	SP
566	NA	**Committed Annual Plan 3 - 30% of servers**	**Wed 01 Dec '10**	**350 days**	**Fri 30 Mar '12**		
567	Wed 01 Dec '10	Refine and Approve Third Committed Annual Plan of the Multi-Year Plan	Wed 01 Dec '10	2 mons	Fri 21 Jan '11		SP
568	NA	**Refine and Approve Third Committed Annual Plan of the Multi-Year Plan**	**Wed 01 Dec '10**	**2 mons**	**Fri 21 Jan '11**	**567SS**	**Prov**
569	NA	**Committed Annual Plan 3 Wave 1**	**Mon 24 Jan '11**	**114 days**	**Thu 30 Jun '11**		
570	NA	Order HW/SW for wave	Mon 24 Jan '11	1 day	Mon 24 Jan '11	567	SP
571	NA	Develop Detailed Plan for migration wave	Fri 04 Feb '11	1 mon	Thu 03 Mar '11	574SS-2 mons	SP
572	NA	Approve Detailed Plan for migration wave	Thu 03 Mar '11	0 days	Thu 03 Mar '11	571	Prov
573	NA	Install and configure HW/SW before migration wave	Tue 22 Feb '11	1 mon	Mon 21 Mar '11	570FS+1 mon	SP
574	NA	Execute migration plan to Calgary DC or Province DC or Interior DC	Fri 01 Apr '11	65 days	Thu 30 Jun '11	565	SP
575	NA	**Committed Annual Plan 3 Wave 2**	**Fri 08 Apr '11**	**126 days**	**Fri 30 Sep '11**		
576	NA	Client consultation to re-confirm wave content	Fri 08 Apr '11	1 mon	Thu 05 May '11	582SS-3 mons	SP
577	NA	Re-confirm wave content	Thu 05 May '11	0 days	Thu 05 May '11	576	Prov
578	NA	Order HW/SW for wave	Fri 06 May '11	1 day	Fri 06 May '11	577	SP
579	NA	Develop Detailed Plan for migration wave	Fri 06 May '11	1 mon	Thu 02 Jun '11	582SS-2 mons	SP
580	NA	Approve Detailed Plan for migration wave	Thu 02 Jun '11	0 days	Thu 02 Jun '11	579	Prov
581	NA	Install and configure HW/SW before migration wave	Mon 06 Jun '11	1 mon	Fri 01 Jul '11	578FS+1 mon	SP
582	NA	Execute migration plan to Calgary DC or Interior DC	Fri 01 Jul '11	66 days	Fri 30 Sep '11	574	SP
583	NA	**Committed Annual Plan 3 Wave 3**	**Mon 11 Jul '11**	**125 days**	**Fri 30 Dec '11**		
584	NA	Client consultation to re-confirm wave content	Mon 11 Jul '11	1 mon	Fri 05 Aug '11	590SS-3 mons	SP
585	NA	Re-confirm wave content	Fri 05 Aug '11	0 days	Fri 05 Aug '11	584	Prov
586	NA	Order HW/SW for wave	Mon 08 Aug '11	1 day	Mon 08 Aug '11	585	SP
587	NA	Develop Detailed Plan for migration wave	Mon 08 Aug '11	1 mon	Fri 02 Sep '11	590SS-2 mons	SP
588	NA	Approve Detailed Plan for migration wave	Fri 02 Sep '11	0 days	Fri 02 Sep '11	587	Prov

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
589	NA	Install and configure HW/SW before migration wave	Tue 06 Sep '11	1 mon	Mon 03 Oct '11	586FS+1 mon	SP
590	NA	Execute migration plan to Calgary DC or Interior DC	Mon 03 Oct '11	65 days	Fri 30 Dec '11	582	SP
591	NA	**Committed Annual Plan 3 Wave 4**	**Mon 10 Oct '11**	**125 days**	**Fri 30 Mar '12**		
592	NA	Client consultation to re-confirm wave content	Mon 10 Oct '11	1 mon	Fri 04 Nov '11	598SS-3 mons	SP
593	NA	Re-confirm wave content	Fri 04 Nov '11	0 days	Fri 04 Nov '11	592	Prov
594	NA	Order HW/SW for wave	Mon 07 Nov '11	1 day	Mon 07 Nov '11	593	SP
595	NA	Develop Detailed Plan for migration wave	Mon 07 Nov '11	1 mon	Fri 02 Dec '11	598SS-2 mons	SP
596	NA	Approve Detailed Plan for migration wave	Fri 02 Dec '11	0 days	Fri 02 Dec '11	595	Prov
597	NA	Install and configure HW/SW before migration wave	Tue 06 Dec '11	1 mon	Mon 02 Jan '12	594FS+1 mon	SP
598	NA	Execute migration plan to Calgary DC or Interior DC	Mon 02 Jan '12	65 days	Fri 30 Mar '12	590	SP
599	NA	**Committed Annual Plan 4 - 20% of servers + 4 "Migration-Only" Waves**	**Thu 01 Dec '11**	**347 days**	**Fri 29 Mar '13**		
600	Thu 01 Dec '11	Refine and Approve Fourth Committed Annual Plan of the Multi-Year Plan	Thu 01 Dec '11	2 mons	Wed 25 Jan '12		SP
601	NA	**Refine and Approve Fourth Committed Annual Plan of the Multi-Year Plan**	**Thu 01 Dec '11**	**2 mons**	**Wed 25 Jan '12**	**600SS**	**Prov**
602	NA	**Committed Annual Plan 4 Wave 1 (includes "Migration-Only" Wave 1)**	**Thu 26 Jan '12**	**112 days**	**Fri 29 Jun '12**		
603	NA	Order HW/SW for wave	Thu 26 Jan '12	1 day	Thu 26 Jan '12	600	SP
604	NA	Develop Detailed Plan for migration wave	Mon 06 Feb '12	1 mon	Fri 02 Mar '12	607SS-2 mons	SP
605	NA	Approve Detailed Plan for migration wave	Fri 02 Mar '12	0 days	Fri 02 Mar '12	604	Prov
606	NA	Install and configure HW/SW before migration wave	Fri 24 Feb '12	1 mon	Thu 22 Mar '12	603FS+1 mon	SP
607	NA	Execute migration plan to Calgary DC or Interior DC	Mon 02 Apr '12	65 days	Fri 29 Jun '12	598	SP
608	NA	**Committed Annual Plan 4 Wave 2 (includes "Migration-Only" Wave 2)**	**Mon 09 Apr '12**	**125 days**	**Fri 28 Sep '12**		
609	NA	Client consultation to re-confirm wave content	Mon 09 Apr '12	1 mon	Fri 04 May '12	615SS-3 mons	SP
610	NA	Re-confirm wave content	Fri 04 May '12	0 days	Fri 04 May '12	609	Prov
611	NA	Order HW/SW for wave	Mon 07 May '12	1 day	Mon 07 May '12	610	SP
612	NA	Develop Detailed Plan for migration wave	Mon 07 May '12	1 mon	Fri 01 Jun '12	615SS-2 mons	SP
613	NA	Approve Detailed Plan for migration wave	Fri 01 Jun '12	0 days	Fri 01 Jun '12	612	Prov
614	NA	Install and configure HW/SW before migration wave	Tue 05 Jun '12	1 mon	Mon 02 Jul '12	611FS+1 mon	SP
615	NA	Execute migration plan to Calgary DC or Interior DC	Mon 02 Jul '12	65 days	Fri 28 Sep '12	607	SP
616	NA	**Committed Annual Plan 4 Wave 3 (includes "Migration-Only" Wave 3)**	**Mon 09 Jul '12**	**126 days**	**Mon 31 Dec '12**		
617	NA	Client consultation to re-confirm wave content	Mon 09 Jul '12	1 mon	Fri 03 Aug '12	623SS-3 mons	SP
618	NA	Re-confirm wave content	Fri 03 Aug '12	0 days	Fri 03 Aug '12	617	Prov
619	NA	Order HW/SW for wave	Mon 06 Aug '12	1 day	Mon 06 Aug '12	618	SP
620	NA	Develop Detailed Plan for migration wave	Mon 06 Aug '12	1 mon	Fri 31 Aug '12	623SS-2 mons	SP
621	NA	Approve Detailed Plan for migration wave	Fri 31 Aug '12	0 days	Fri 31 Aug '12	620	Prov
622	NA	Install and configure HW/SW before migration wave	Tue 04 Sep '12	1 mon	Mon 01 Oct '12	619FS+1 mon	SP
623	NA	Execute migration plan to Calgary DC or Interior DC	Mon 01 Oct '12	66 days	Mon 31 Dec '12	615	SP
624	NA	**Committed Annual Plan 4 Wave 4 (includes "Migration-Only" Wave 4)**	**Tue 09 Oct '12**	**124 days**	**Fri 29 Mar '13**		
625	NA	Client consultation to re-confirm wave content	Tue 09 Oct '12	1 mon	Mon 05 Nov '12	631SS-3 mons	SP
626	NA	Re-confirm wave content	Mon 05 Nov '12	0 days	Mon 05 Nov '12	625	Prov
627	NA	Order HW/SW for wave	Tue 06 Nov '12	1 day	Tue 06 Nov '12	626	SP
628	NA	Develop Detailed Plan for migration wave	Tue 06 Nov '12	1 mon	Mon 03 Dec '12	631SS-2 mons	SP
629	NA	Approve Detailed Plan for migration wave	Mon 03 Dec '12	0 days	Mon 03 Dec '12	628	Prov
630	NA	Install and configure HW/SW before migration wave	Wed 05 Dec '12	1 mon	Tue 01 Jan '13	627FS+1 mon	SP

ID	Constraint Date	Task Name	Start	Duration	Finish	Predecessors	Resource Names
631	NA	Execute migration plan to Calgary DC or Interior DC	Tue 01 Jan '13	64 days	Fri 29 Mar '13	623	SP
632	NA	**Committed Annual Plan 5 - 20 % of servers + 3 "M-O" Waves + "Unrefreshable" Servers**	**Mon 03 Dec '12**	**346 days**	**Mon 31 Mar '14**		
633	Sat 01 Dec '12	Refine and Approve Fifth Committed Annual Plan of the Multi-Year Plan	Mon 03 Dec '12	2 mons	Fri 25 Jan '13		SP
634	NA	**Refine and Approve Fifth Committed Annual Plan of the Multi-Year Plan**	**Mon 03 Dec '12**	**2 mons**	**Fri 25 Jan '13**	**633SS**	**Prov**
635	NA	**Committed Annual Plan 5 Wave 1 (includes "Migration-Only" Wave 5)**	**Mon 28 Jan '13**	**110 days**	**Fri 28 Jun '13**		
636	NA	Order HW/SW for wave	Mon 28 Jan '13	1 day	Mon 28 Jan '13	634	SP
637	NA	Develop Detailed Plan for migration wave	Mon 04 Feb '13	1 mon	Fri 01 Mar '13	640SS-2 mons	SP
638	NA	Approve Detailed Plan for migration wave	Fri 01 Mar '13	0 days	Fri 01 Mar '13	637	Prov
639	NA	Install and configure HW/SW before migration wave	Tue 26 Feb '13	1 mon	Mon 25 Mar '13	636FS+1 mon	SP
640	NA	Execute migration plan to Calgary DC or Interior DC	Mon 01 Apr '13	65 days	Fri 28 Jun '13	631	SP
641	NA	**Committed Annual Plan 5 Wave 2 (includes "Migration-Only" Wave 6)**	**Mon 08 Apr '13**	**126 days**	**Mon 30 Sep '13**		
642	NA	Client consultation to re-confirm wave content	Mon 08 Apr '13	1 mon	Fri 03 May '13	648SS-3 mons	SP
643	NA	Re-confirm wave content	Fri 03 May '13	0 days	Fri 03 May '13	642	Prov
644	NA	Order HW/SW for wave	Mon 06 May '13	1 day	Mon 06 May '13	643	SP
645	NA	Develop Detailed Plan for migration wave	Mon 06 May '13	1 mon	Fri 31 May '13	648SS-2 mons	SP
646	NA	Approve Detailed Plan for migration wave	Fri 31 May '13	0 days	Fri 31 May '13	645	Prov
647	NA	Install and configure HW/SW before migration wave	Tue 04 Jun '13	1 mon	Mon 01 Jul '13	644FS+1 mon	SP
648	NA	Execute migration plan to Calgary DC or Interior DC	Mon 01 Jul '13	66 days	Mon 30 Sep '13	640	SP
649	NA	**Committed Annual Plan 5 Wave 3 (includes "Migration-Only" Wave 7)**	**Tue 09 Jul '13**	**126 days**	**Tue 31 Dec '13**		
650	NA	Client consultation to re-confirm wave content	Tue 09 Jul '13	1 mon	Mon 05 Aug '13	656SS-3 mons	SP
651	NA	Re-confirm wave content	Mon 05 Aug '13	0 days	Mon 05 Aug '13	650	Prov
652	NA	Order HW/SW for wave	Tue 06 Aug '13	1 day	Tue 06 Aug '13	651	SP
653	NA	Develop Detailed Plan for migration wave	Tue 06 Aug '13	1 mon	Mon 02 Sep '13	656SS-2 mons	SP
654	NA	Approve Detailed Plan for migration wave	Mon 02 Sep '13	0 days	Mon 02 Sep '13	653	Prov
655	NA	Install and configure HW/SW before migration wave	Wed 04 Sep '13	1 mon	Tue 01 Oct '13	652FS+1 mon	SP
656	NA	Execute migration plan to Calgary DC or Interior DC	Tue 01 Oct '13	66 days	Tue 31 Dec '13	648	SP
657	NA	**Committed Annual Plan 5 Wave 4 (includes physically "unresfreshable servers", if an**	**Wed 09 Oct '13**	**124 days**	**Mon 31 Mar '14**		
658	NA	Client consultation to re-confirm wave content	Wed 09 Oct '13	1 mon	Tue 05 Nov '13	664SS-3 mons	SP
659	NA	Re-confirm wave content	Tue 05 Nov '13	0 days	Tue 05 Nov '13	658	Prov
660	NA	Order HW/SW for wave	Wed 06 Nov '13	1 day	Wed 06 Nov '13	659	SP
661	NA	Develop Detailed Plan for migration wave	Wed 06 Nov '13	1 mon	Tue 03 Dec '13	664SS-2 mons	SP
662	NA	Approve Detailed Plan for migration wave	Tue 03 Dec '13	0 days	Tue 03 Dec '13	661	Prov
663	NA	Install and configure HW/SW before migration wave	Thu 05 Dec '13	1 mon	Wed 01 Jan '14	660FS+1 mon	SP
664	NA	Execute migration plan to Calgary DC or Interior DC	Wed 01 Jan '14	64 days	Mon 31 Mar '14	656	SP
665	NA	Migrate physical "unrefreshable" servers (plan assumes there are none)	Mon 30 Dec '13	66 days	Mon 31 Mar '14	664FF	SP

SCHEDULE 11

SERVICE LEVELS

(Section 8.9)

1. **Purpose**. This purpose of this Schedule is to describe the Service Levels that the Service Provider will achieve in performing the Services.

2. **Appendices**. The following Appendices attached to this Schedule are incorporated into this Schedule by reference:

(a) Appendix 11–A (*Service Level Measurements*), which sets forth the quantitative measurements associated with SLA's and SLOs. The Service Provider shall perform the Services at or above the levels of performance indicated in Appendix 11–A (*Service Level Measurements*);

(b) Appendix 11–B (*Service Level Descriptions and Definitions*), which sets forth the descriptions and definitions for the SLAs and SLO's identified in Appendix 11–A (Service Level Measurements); and

(c) Appendix 11–C (*Data Center Service Levels*), which provides the Service Levels, Service Level Credits and associated terms and conditions for the STMS Data Center Services. The Service Provider shall perform the STMS Data Center Services at or above the levels of performance described in Appendix 11–C (*Data Center Service Levels*), but subject to the provisions of Section 7 (*STMS Data Centre Services*) below.

3. **Definitions**. Where used in this Schedule, the following words will have the meanings set forth below, and any other words defined in this Schedule will have the meanings so given to them:

(a) "**Actual Uptime**" means the measurement of time that a particular Supported Infrastructure or any other part of the Services is actually available during the applicable Measurement Window, calculated by subtracting Downtime from the Scheduled Uptime;

(b) "**Availability**" means the Actual Uptime expressed as a percentage of the Scheduled Uptime for a particular item or group of items within the Supported Infrastructure (i.e., Availability % = ((Actual Uptime)/(Scheduled Uptime)) x 100);

(c) "**Downtime**" means the time that a particular item or group of items within the Supported Infrastructure is not available during the applicable Measurement Window, and for purposes of calculating such "Downtime", the period of time that is outside of the Service Provider's control, as determined by a root cause analysis for the Incident, will not be applied to the SLA or SLO impacted by the Incident.

(d) "**Measurement Window**" means the time during, or frequency by, which a Service Level is measured, and is calculated as the Support Hours less the Scheduled Downtime;

(e) "**Scheduled Downtime**" means that period of time (measured by hours and minutes of the day) during which a particular item or group of items in the Supported Infrastructure is scheduled to be unavailable for maintenance and other similar purposes, and includes any of the following that may occur during the Support Hours:

(i) scheduled change windows, for the particular item or group of items in the Supported Infrastructure, that are used by the Service Provider to perform maintenance or other scheduled downtime activities;

(ii) and other downtime that is agreed to through the Change Management Process; and

(iii) Client initiated downtime including operational reboots.

(f) "**Scheduled Uptime**" means that period of time (measured by days of the week, and hours and minutes of the day) during which a particular item or group of items in the Supported Infrastructure is expected to be available during the Measurement Window, calculated as the Support Hours less the Scheduled Downtime;

(g) "**Service Level**" means the desired level of performance set forth in Appendix 11–A (*Service Level Measurements*) and Appendix 11–B (*Service Level Descriptions and Definitions*);

(h) "**Service Level Agreement**" or "**SLA**" means those Service Levels established under this Schedule for which a Service Level Credit may be payable; and

(i) "**Service Level Objective**" or "**SLO**" means those Service Levels established under this Schedule for which no Service Level Credit is payable

(j) "**Support Hours**" means that period of time (measured by days of the week, and hours and minutes of the day) during which a particular item or group of items in the Supported Infrastructure is supported by the Service Provider, as set forth in the "Support Hours" column of Appendix 11–A (*Service Level Measurements*), calculated as follows:

(i) 5x9 is from 8:00 AM to 5:00 PM during each Business Day;

(ii) 5x12 is 7:00 AM to 7:00 PM during each Business Day;

(iii) 7x24 is all day every day.

4. **Commencement of Obligations**. The Service Levels set forth in Appendix 11–A (*Service Level Measurements*) and Appendix 11–B (*Service Level Descriptions and Definitions*):

(a) for all Service Level categories except Mainframe shall commence on the dates specified in Appendix 11–A (*Service Level Measurements*) as set referenced in the column titled "CD + mos" as applicable, where the numbers used in that column are in the format X, where "X" represents the number of months after the Hand-Over Date when the Service Provider will be responsible to provide the Province with measurement data in support of the SLAs, for achieving the SLAs, and for any SLA Failures; and

(b) for the Mainframe Service Level categories shall commence on the dates specified in Appendix 11–A (*Service Level Measurements*) as set referenced in the column titled "MF + mos" as applicable, where the numbers used in that column are in the format X, where "X" represents the number of months after the Mainframe Transformation (which must occur by January 31, 2011), and when the Service Provider will be responsible to provide the Province with measurement data in support of the Mainframe SLAs, for achieving the Mainframe SLAs, and for any Mainframe SLA Failures.

5. **Existing Equipment**. During the first six (6) months following the Hand-Over Date, the Service Provider will review the Initial Supported Infrastructure (as defined in the Security SOW) to determine whether there are any existing technical design issues in respect of such Initial Supported Infrastructure that would prevent the Service Provider from achieving the SLAs or SLOs (as applicable) in respect of such Initial Supported Infrastructure.

If the Service Provider establishes to the reasonable satisfaction of the Province that such technical design issues exist which will prevent the Service Provider from achieving any applicable SLA and SLOs (the "**Subject Service Levels**") on specific components of the Initial Supported Infrastructure (the "**Restricted Infrastructure**"), then the Subject Service Levels shall not apply to the Restricted Infrastructure. The parties will work together to determine the manner in which they will address the Restricted Infrastructure and any remedies that the Province may wish to apply to such Restricted Infrastructure, and if they are unable to agree, then either Party may refer the matter to Governance for resolution. Except as set forth above regarding the Restricted Infrastructure and the Subject Service Levels, the Service Levels shall apply to all Initial Supported Infrastructure commencing in the seventh (7th) month following the Hand-Over Date.

The time period in which the Service Provider may determine that there is Restricted Infrastructure to which the Subject Service Levels do not apply is not limited to the first six (6) months after the Hand-Over Date. For greater clarification, if the Service Provider establishes that there is additional Restricted Infrastructure (the "**Additional Restricted Infrastructure**") after such six (6) period (the date upon which it is so established being referred to as the "**Delayed Restriction Date**"), then the Additional Restricted Infrastructure shall still be subject to the Service Levels from the seventh (7th) month following the Hand-Over Date until the Delayed Restriction Date.

6. **Service Levels Measured by Percentage.** Some Service Levels are expressed as achieving a level of performance over a percentage of items occurring during a Measurement Window. If the number of items occurring during a given Measurement Window is less than or equal to 100, then the following algorithm will be used to determine the number of compliant items that the Service Provider must successfully complete to achieve the applicable Service Level (the "**Minimum Compliant Items**"):

(a) the number of items occurring during the Measurement Window shall be multiplied by the Service Level Target; and

(b) if the product of that multiplication is not a whole number, then such product shall be truncated to a whole number.

For example, if a Service Level requires the completion of 95% of incidents within 4 hours to achieve the Service Level, then:

(i) if the number of incidents is 100, then the Minimum Compliant Items is 95 incidents in a 4 hour period (100 incidents x 95% = 95 incidents);

(ii) if the number of incidents is 99, then the Minimum Compliant Items is 94 incidents in a 4 hour period (99 incidents x 95% = 94.05 incidents, truncated to 94); and

(iii) if the number of incidents is 9, then the Minimum Compliant Items is 8 incidents in a 4 hour period (9 incidents x 95% = 8.55 incidents, truncated to 8).

7. **STMS Data Centre Services.** The Service Provider will perform the STMS Data Centre Services in accordance with the Service Levels set forth in Appendix 11–C (*Data Center Service Levels*). The calculation of any DC Service Level Credits in respect of the Data Centre SLAs will be made in accordance with the provisions of Appendix 11–C (Data Center Service Levels).

8. **Reporting.** Commencing in the seventh (7th) month after the Hand-Over Date, the Service Provider will provide the Province with monthly reporting on the Service Levels described in Appendix 11–A (*Service Level Measurements*) and Appendix 11–B (*Service Level Descriptions and Definitions*), on a Client Organization basis (as defined in the Services management SOW), using the format specified in Appendix 11-D (*Reports*) of this Schedule. The Service Provider will provide the Province with reporting on the Service Levels described in Appendix 11–C (*Data Center Service Levels*) at the times and in the manner set forth in Appendix 11–C (*Data Center Service Levels*).

APPENDIX 11-A

SERVICE LEVEL MEASUREMENTS

This Appendix 11-A (*Service Level Measurements*) sets forth the following:

(a) for Service Level Agreements (SLAs):

(i) the numeric measurements for each SLA;

(ii) the basis for the numeric measurement (such as Average, Percentage, Per Cluster);

(iii) the Weighting associated with the SLA;

(iv) the timing for when the Service Provider's obligations in respect of the SLA, and reporting on the SLA, commence; and

(v) cross references to Appendix 11–B (*Service Level Descriptions and Definitions*) where the qualitative description of the SLAs can be found; and

(b) for Service Level Objectives (SLOs):

(i) the numeric measurements for each SLO;

(ii) the timing for when the Service Provider's obligations in respect of the SLO, and reporting on the SLO, commence; and

(iii) cross references to Appendix 11–B (*Service Level Descriptions and Definitions*) where the qualitative description of the SLOs can be found.

In the SLO Table below, the following apply:

S. 15

IMS Transaction Classes				
Class	CPU (seconds)	# of DLI calls	# of physical I/Os	Resource Objective
1	≤ 0.0075	≤ 10	≤ 5	99.5% completed in 2 seconds
2	≤ 0.0124	≤ 25	≤ 12	99.5% completed in 3 seconds
3	≤ 0.0172	≤ 50	≤ 25	99.5% completed in 5 seconds

TSO Transaction Classes		
Class	Target Volume	Resource Objective
1	80%	98% completed in 2 seconds
2	10%	98% completed in 3 seconds
3	8%	98% completed in 5 seconds

Batch Completion Rates	
Class	Resource Objective
5	100% completed by 07:00 the next business day
6	99.9% completed by 07:00 the next business day if submitted between 18:00-21:00

At Risk Pool Available									**250%**
At Risk Pool Available Unallocated — Expressed as % of the pool not allocated									**0%**
Appendix 11-B Section Reference	**Service Level Agreements (SLAs)**						**Measurement**		**70.0%**
1	**Performance Category - Midrange**	**CD + mos (2)**	**Service Level Target**	**Maximum SLA Target (3)**	**SLA Basis**	**SLA Group**	**Measurement Frequency**	**Support Hours**	**Weightings (1)**
1.1	Tier 1 - Business Priority - Geographically Distributed Cluster Availability (synchronous data replication)	6	99.90%	99.999%	Per Cluster	MR-A	Monthly	7x24	20.0%
1.2	Tier 1 - Business Priority - Geographically Distributed Cluster Availability (asynchronous data replication)	6	99.90%	99.99%	Per Cluster	MR-A	Monthly	7x24	0.0%
1.3	Tier 1 - Business Priority - Clustered Server Datacentre Located Availability	6	99.90%	99.95%	Per Cluster	MR-A	Monthly	7x24	20.0%
1.4	Tier 2 - General Business - Province Datacentre Server Availability	6	99.70%	n/a	Average	MR-A	Monthly	7x24 (4)	15.0%
1.5	Tier 2 - General Business - STMS Datacentre Server Availability	6	99.70%	n/a	Per Server	MR-A	Monthly	7x24 (4)	15.0%

Appendix 11-B Section Reference	**Service Level Agreements (SLAs)**						**Measurement**		**45.0%**
2	**Performance Category - Storage**	**CD + mos (2)**	**Service Level Target**	**Maximum SLA Target (3)**	**SLA Basis**	**SLA Group**	**Measurement Window**	**Support Hours**	**Weightings (1)**
2.1	Tier 1- Mission Critical Storage Availability	6	99.999%	n/a	Average	SB-A	Monthly	7x24	20.0%
2.2	Tier 2&3 - Business Priority Storage Availability	6	99.95%	n/a	Average	SB-A	Monthly	7x24	15.0%
2.3	Backup - Successful Completion of Backups	6	95.00%	n/a	Percentage	SB-B	Monthly	7x24	5.0%
2.4	Restores - Time to Initiate Restore within 30 minutes (when tape is in silo)	6	90.00%	n/a	Percentage	SB-B	Monthly	7x24	5.0%

At Risk Pool Available									250%
At Risk Pool Available Unallocated -- Expressed as % of the pool not allocated									0%
Appendix 11-B Section Reference	Service Level Agreements (SLAs)						Measurement		70.0%
1	Performance Category - Midrange	CD + mos (2)	Service Level Target	Maximum SLA Target (3)	SLA Basis	SLA Group	Measurement Frequency	Support Hours	Weightings (1)
Appendix 11-B Section Reference	Service Level Agreements (SLAs)						Measurement		10.0%
3	Performance Category - Cross Functional	CD + mos (2)	Service Level Target	Maximum SLA Target (3)	SLA Basis	SLA Group	Measurement Window	sSupport Hours	Weightings (1)
3.1	Responses to Priority 1 Incident within target	6	90.00%	n/a	Percentage	n/a	Monthly	7x24	5.0%
3.2	Responses to Priority 2 Incident within target	6	90.00%	n/a	Percentage	n/a	Monthly	7x24	5.0%
Appendix 11-B Section Reference	Service Level Agreements (SLAs)						Measurement	%	125.0%
4	Performance Category - Mainframe	MF + mos (2A)	Service Level Target	Interrupt Count (3A)	SLA Basis	SLA Group	Measurement Window	Support Hours	Weightings (1)
4.1	Mainframe Availability - OS - System A	3	99.80%	≤ 2	Average	MF-A	Monthly	7x24	20.0%
4.2	Mainframe Availability - OS - System I	3	99.80%	≤ 2	Average	MF-A	Monthly	7x24	20.0%
4.3	Mainframe Availability - CICS	3	99.80%	≤ 1 per region	Per Region (5)	MF-A	Monthly	7x24	20.0%
4.4	Mainframe Availability - DB2	3	99.80%	≤ 2	Per Region (5)	MF-A	Monthly	7x24	20.0%
4.5	Mainframe Availability - IMS	3	99.80%	≤ 2	Per Region (5)	MF-A	Monthly	7x24	20.0%

At Risk Pool Available									250%
At Risk Pool Available Unallocated -- Expressed as % of the pool not allocated									0%
Appendix 11-B Section Reference	Service Level Agreements (SLAs)						Measurement		70.0%
1	Performance Category - Midrange	CD + mos (2)	Service Level Target	Maximum SLA Target (3)	SLA Basis	SLA Group	Measurement Frequency	Support Hours	Weightings (1)
4.6	Mainframe Availability - MQ	3	99.80%	≤ 2	Per Region (5)	MF-A	Monthly	7x24	15.0%
4.7	IMS Class 2 Performance	3	99.50%	n/a	Percentage	MF-B	Monthly	7x24	5.0%
4.8	Batch Class 7 Performance	7	99.50%	n/a	Percentage	MF-B	Monthly	7x24	5.0%
TOTAL									250%

Notes	
(1)	See Schedule 12 - Service Level Failures for the definition of Weightings
(2)	Number of months after Commencement Date when the Service Provider is responsible for Service Level performance and Service Level Credits due for Service Level Defaults.
(2A)	Number of months after Mainframe Transformation when the Service Provider is responsible for Service Level performance and Service Level Credits due for Service Level Defaults
(3)	If a Maximum SLA Target is specified then, the Service Level Target is to be reviewed annual, starting at month 1, and raised by one-half the distance between the then current target and the actual achievement to a maximum of the Maximum SLA Target
(3A)	If the number of interrupts is exceeded then the Service Level Target is considered as not achieved
(4)	Some Servers in this group may have 5x9 or 5x12 Support Hours
(5)	1 region in every 10 allowed 2 hours 54 minutes outage time

Appendix 11-B Section Reference	Service Level Objectives (SLOs)						
5	**Performance Category - Midrange**	**CD + mos (7A)**	**Service Level Target**	**SLA Basis**	**SLA Group**	**Measurement Window**	**Support Hours**
5.1	Tier 2 - General Business - Aged Infrastructure Availability	6	99.50%	Per Server	n/a	Monthly	7x24 (9)
5.2	Tier 3 - Remote Server Availability	6	99.70%	Average	MR-B (6A)	Monthly	7x24
5.3	Midrange Provisioning - Standard Physical Server (within 4 weeks)	6	80.00%	Percentage	n/a	Annually	5x9
5.4	Midrange Provisioning - Custom Physical Server (within 8 weeks)	6	80.00%	Percentage	n/a	Annually	5x9
5.5	Midrange Provisioning - Standard Virtual Server (within 3 Days)	6	80.00%	Percentage	n/a	Annually	5x9
6	**Performance Category - Storage**	**CD + mos (7A)**	**Service level Target**	**SLA Basis**	**SLA Group**	**Measurement Window**	**Support Hours**
6.1	Time to Provision Storage	6	90.00%	Percentage	n/a	Monthly	7x24
7	**Performance Category - Cross functional**	**CD + mos (7A)**	**Service Level Target**	**SLA Basis**	**SLA Group**	**Measurement Window**	**Support Hours**
7.1	Response to Priority 3 Incident within target	6	90.00%	Percentage	n/a	Monthly	5x8
7.2	Response to Priority 4 Incident within target	6	90.00%	Percentage	n/a	Monthly	5x8
7.3	Update to Priority 1 Incident within target	6	90.00%	Percentage	n/a	Monthly	7x24
7.4	Update to Priority 2 Incident within target	6	90.00%	Percentage	n/a	Monthly	7x24
7.5	Change Management - Successful Changes	6	75.00%	Percentage	MR-B (6A)	Monthly	7x24

8	Performance Category – Mainframe (8)	MF + mos (7B)	Service Level Target	SLA Basis	SLA Group	Measurement Window	Support Hours
8.1	CICS transaction speed measured by customer application summary set completion	3	97.00%	Percentage	n/a	Monthly	7x24
8.2	IMS transaction speed per defined IMS transaction classes (8)	3	99.50%	Percentage	n/a	Monthly	7x24
8.3	TSO transaction speed per defined TSO transaction classes	3	98.00%	Percentage	n/a	Monthly	7x24
8.4	Batch complettion rates per defined batch job classes Class 5 (weekend) Class 6 (overnight) Class 7 (see SLAs) Class 8 (12 minutes) Class 9 (6 minutes)	3	 100% 99.9 see SLAs 90.0 96.2	Percentage	n/a	Monthly	7x24
9	Performance Category - Service Desk	CD + mos (7A)	Service Level Target		SLA Group	Measurement Window	Support Hours
9.1	Service Desk Speed to Answer	6	25.00%	Percentage	n/a	Monthly	Weekdays 6pm - 6am; weekends and holidays 24 hours
9.2	Service Desk Incident Creation within target	6	90.00%	Percentage	n/a	Monthly	Weekdays 6pm - 6am; weekends and holidays 24 hours

Notes:	
(6)	Service Level Target to be re-evaluated after 12 months
(6A)	SLA Group applied if promoted to SLA; SLOs do not count towards an SLA Termination Event

Notes:	
(7A)	Number of months after Commencement Date when Service Provider is responsible for Service Level performance
(7B)	Number of months after Mainframe Transformation when the Service Provider is responsible for Service Level performance
(8)	Excludes IMS class 2 (see Critical Service Levels)
(8A)	The Mainframe SLOs currently include production regions only.
(9)	Some servers in this group may have 5x9 or 5x12 Support Hours

APPENDIX 11-B

SERVICE LEVEL DEFINITIONS AND DESCRIPTIONS

SERVICE LEVEL AGREEMENTS (SLA)

This Section sets forth qualitative descriptions of the Service Level Agreements (SLAs). The numerical Service Level Targets, Measurement Windows, Support Hours and commencement of obligations associated with such SLAs are set forth in Appendix 11–A (Service Level Measurements).

1. PERFORMANCE CATEGORY – MIDRANGE AVAILABILITY

Midrange Availability Calculation Summary.

The general approach for midrange measurements is described in this Section 1.

The Supported Infrastructure for the Midrange SOWs are considered available when their Operating System is available to the user network (at the Service Provider network demark). Responsibility for Application recovery resides with the Province.

The calculation for clustered Server systems availability is based on availability of the network Operating System from a system that is made up of many server nodes. The entire clustered system is considered available once the network operating system of the system is available to the user network regardless of the status of any individual server node.

1.1 Tier 1 - Business Priority - Geographically Distributed Cluster Availability (Synchronous Data Replication)

This Tier synchronously replicates data between two or more data centres for the purpose of maintaining an active clustered server and associated data. Synchronously replicated data essentially maintains identical datasets concurrently. A geographically distributed cluster is a group of linked servers (nodes) located in two or more geographically distributed datacentres. The linked servers (the cluster) act as a single system. Servers in this Tier can be virtual or physical servers but not mixed. All nodes in the cluster have to be identical servers (i.e. the same operating system and hardware of comparable performance).

Notes:

(a) This Tier requires the Tier 1 Storage and Optional services Local Clone and Replication from the Storage Services for the application and application related data.

(b) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLA.

(c) If the Parties are unable to agree on the manner in which any Tier 1 Restricted Infrastructure will be handled on a case by case basis, then the default approach will be to demote the Tier 1 Restricted Infrastructure to Tier 2.

(d) This SLA requires that the network latency meets or is better than the level required for synchronous data replication as recommended by the storage replication vendor.

(e) **Availability Percentage Calculation**: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (*Midrange Availability Calculation*);

(f) **Compliance Calculation**: The Availability will be calculated on each Cluster in this Tier 1 category separately. The SLA will be achieved if all Clusters have an Availability greater than or equal to the Service Level Target.

1.2 **Tier 1 - Business Priority - Geographically Distributed Cluster Availability (asynchronous data replication).**

This Tier asynchronously replicates data between two or more data centres for the purpose of maintaining an active clustered server and associated data. Asynchronously replicated data essentially maintains identical datasets with some time lag. The time lag is typically measured in seconds or minutes. A Geographically distributed cluster is a group of linked servers (nodes) between two or more geographical data centres (i.e. two or more data centers). The linked servers act as a single system. Servers in this Tier can be virtual or physical servers but not mixed. All nodes in the cluster have to be identical servers (i.e. the same operating system and hardware of comparable performance).

Notes:

(a) This Tier requires the Tier 1 Storage and Optional services Local Clone and Replication from the Storage Services for the application and application related data.

(b) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLA.

(c) If the Parties are unable to agree on the manner in which any Tier 1 Restricted Infrastructure will be handled on a case by case basis, then the default approach will be to demote the Tier 1 Restricted Infrastructure to Tier 2..

(d) **Availability Percentage Calculation**: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (*Midrange Availability Calculation*);

(e) **Compliance Calculation**: The Availability will be calculated on each Cluster in this Tier 1 category separately. The SLA will be achieved if all Clusters have an Availability greater than or equal to the Service Level Target.

1.3 **Tier 1 – Business Priority – Clustered Server Datacentre Located Availability.**

A single site cluster is a group of linked servers in a single data center. The linked servers (nodes) act as a single system. Servers in this Tier can be virtual or physical servers but not mixed. All nodes in the cluster have to be identical servers (i.e. the same operating system and hardware of comparable performance).

Notes:

(a) This Tier requires the Tier 2 Storage from the Storage Services for the application and application related data.

(b) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLA.

(c) If the Parties are unable to agree on the manner in which any Tier 1 Restricted Infrastructure will be handled on a case by case basis, then the default approach will be to demote the Tier 1 Restricted Infrastructure to Tier 2.

(d) **Availability Percentage Calculation**: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (*Midrange Availability Calculation*);

(e) **Compliance Calculation**: The Availability will be calculated on each Cluster in this Tier 1 category separately. The SLA will be achieved if all Clusters have an Availability greater than or equal to the Service Level Target.

1.4 **Tier 2 - General Business - Province Datacentre Server Availability.**

This Tier is a single server (i.e. non-clustered) in a Province Data Centre (as defined in the Server Management SOW) that either: (1) is part of the Initial Supported Infrastructure at the time of the Hand-Over Date; or (2) is deployed after the commencement of the Committed Annual Plan 1 Wave 1 (Pilot Wave) as more particularly described in of the Transformation SOW (the "Tier 2 Deployment Date"). Servers in this Tier can be virtual or physical servers.

Notes:

(a) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLA.

(b) **Availability Percentage Calculation**: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (*Midrange Availability Calculation*);

(c) **Compliance Calculation**: The Availability will be calculated by aggregating the results of all Servers in this Tier 2 category together to arrive at an average (e.g. the sum of all Actual Uptimes divided by the sum of all Scheduled Uptimes expressed as a percentage). The SLA will be achieved if the average Availability of all Servers is greater than or equal to the Service Level Target.

1.5 **Tier 2 – General Business – STMS Data Centre Server Availability**.

This Tier is a single server (i.e. non-clustered) in: (1) an STMS Data Centre, or (2) in a Province Data Centre that is deployed after the Tier 2 Deployment Date. Servers in this Tier can be virtual or physical servers.

Notes:

(a) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLA.

(b) b: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (Midrange Availability Calculation);

(c) **Compliance Calculation**: The Availability will be calculated on each Server n this Tier 2 category separately. The SLA will be achieved if 98% of Servers have an Availability greater than or equal to the Service Level Target.

2. **PERFORMANCE CATEGORY – STORAGE**

Storage Availability Measurement.

Storage availability measures the availability of the SAN fabric and Storage frames.

2.1 **Tier 1 - Mission Critical Storage Availability.**

(a) **Compliance Calculation**. The Availability will be calculated by aggregating the results of all Storage frames in this Tier 1 category together to arrive at an average (e.g. the sum of all Actual Uptimes for the Storage frames divided by the sum of all Scheduled Uptimes expressed as a percentage). The SLA will be achieved if the average Availability of all Storage frames is greater than or equal to the Service Level Target.

(b) **Exclusions**: Incidents will be excluded from the Downtime where it is determined on a root cause analysis that the Province has not implemented (or approved the implementation of) relevant EMC or third-party recommended patches or firmware.

2.2 **Tier 2 & 3 - Business Priority Storage Availability.**

(a) **Compliance Calculation.** The Availability will be calculated by aggregating the results of all Storage frames in this Tier 2&3 category together to arrive at an average (e.g. the sum of all Actual Uptimes for the Storage frames divided by the sum of all Scheduled Uptimes expressed as a percentage). The SLA will be achieved if the average Availability of all Storage frames is greater than or equal to the Service Level Target.

(b) **Exclusions:** Incidents will be excluded from the Downtime where it is determined on a root cause analysis that the Province has not implemented (or approved the implementation of) relevant EMC or third-party recommended patches or firmware.

2.3 **Backup – Successful Completion of Backups.**

(a) **Compliance Calculation:** Compliance shall be calculated for a given Measurement Window as the ratio of successful backup jobs completed, divided by total number of backup jobs submitted in that Measurement Window with the result expressed as a percentage, and then comparing this percentage to the Service Level Target for this SLA:

2.4 **Restore – Time to Initiate Restore within 30 Minutes (when tape is in silo).**

(a) Time to Initiate Restore shall be measured as the time a Priority 1 restore ticket is created to the time data starts to transfer to the target server.

(b) For shared file and print full image restores Time to Initiate Restore shall be measured as the time a Priority 1 restore ticket is created to the time data starts to transfer to the target nearline storage server (being the replicated copy of the production shared file server data).

(c) **Compliance Calculation:** Compliance shall be measured by dividing the number of Priority 1 restore tickets, where the tape is in the silo, with a Time to Initiate Restore less than or equal to 30 minutes, by the total number of Priority 1 restore tickets, with the result expressed as a percentage, and comparing this percentage to the Service Level Target for this SLA. Any non-backup application related problem, preventing the restore from initiating will be removed from measurement. Time to Initiate Restore within Target is calculated as:

Number of Priority 1 restore tickets (where the tape is in the silo) with a Time to Restore less than or equal to 30 minutes / Total Priority 1 restore tickets (where the tape is in the silo).

3. PERFORMANCE CATEGORY – CROSS FUNCTIONAL

3.1 Response to Priority 1 Incident within Target.

(a) **Response** means the acknowledgement by Service Provider of a Priority 1 Incident assigned by the Province Service Desk. The Service Provider acknowledgement shall be the earlier of:

(i) a verbal acknowledgement recorded by the Province Service Desk; or

(ii) the time that an incident is created in ITIMS in response to notifications about a previously auto-generated and assigned incident.

(b) **Target** means:

(i) fifteen (15) minutes during the hours of 8 AM to 5 PM on Business Days; or

(ii) thirty (30) minutes during the hours of 5 PM to 8 AM during the Support Hours.

(c) **Compliance Calculation:** For any Measurement Window, compliance shall be calculated as the number of Priority 1 Incidents allocated to Service Provider by the Province Service Desk that are responded to within Target, divided by the number of Priority 1 Incidents allocated to the Service Provider, with the result expressed as a percentage to two decimal places, and comparing this percentage to the Service Level Target for this SLA. The SLA is considered achieved if the percentage is greater than or equal to the Service Level Target.

(d) **Exclusion:** For Priority 1 incidents, communication of the Priority 1 assignment from the Province Service Desk to the Service Provider is expected to be completed within a period of time that is equal to 10% of the Target. Incidents where communication is interrupted or delayed by the Province Service Desk will be excluded from compliance calculations.

3.2 Response to Priority 2 Incident within Target.

(a) **Response** means the acknowledgement by Service Provider of a Priority 2 Incident assigned by the Province Service Desk. The Service Provider acknowledgement shall be the earlier of:

(i) a verbal acknowledgement recorded by the Province Service Desk; or

(ii) the time that an incident is created in ITIMS in response to notifications about a previously auto-generated and assigned incident

(b) **Target** means:

(i) thirty (30) minutes during the hours of 8 AM to 5 PM on Business Days; or

(ii) thirty (30) minutes during the hours of 5 PM to 8 AM during the Support Hours.

(c) **Compliance Calculation**: For any Measurement Window, compliance shall be calculated as the number of Priority 2 Incidents allocated to Service Provider by the Province Service Desk that are responded to within Target, divided by the number of Priority 2 Incidents allocated to the Service Provider, with the result expressed as a percentage to two decimal places, and comparing this percentage to the Service Level Target for this SLA. The SLA is considered achieved if the percentage is greater than or equal to the Service Level Target.

(d) **Exclusion:** For Priority 2 incidents, communication of the Priority 2 assignment from the Province Service Desk to the Service Provider is expected to be completed within a period of time that is equal to 10% of the Target. Incidents where communication is interrupted or delayed by the Province Service Desk will be excluded from compliance calculations.

4. PERFORMANCE CATEGORY – MAINFRAME

4.1 Mainframe Availability – OS – System A.

(a) System Availability measurement is from the presentation to the user network at the Service Provider network demark.

(b) **Compliance Calculation:** Mainframe Availability – OS – System A is the Actual Uptime expressed as a percentage of the Scheduled Uptime for the System A Operating System. The SLA is achieved if the Availability is greater than or equal to the Service Level Target for this SLA.

4.2 Mainframe Availability – OS – System I.

(a) System Availability measurement is from the presentation to the user network at the Service Provider network demark.

(b) **Compliance Calculation:** Mainframe Availability – OS – System I is the Actual Uptime expressed as a percentage of the Scheduled Uptime for the System I Operating System. The SLA is achieved if the Availability is greater than or equal to the Service Level Target for this SLA.

4.3 Mainframe Availability – CICS.

(a) Region Availability means the proportion of time a production CICS region is in a functioning and accessible state.

(b) **Calculation**:

(i) **Extended Outage Targets**: one production CICS region in every 10 is allowed an Extended Outage Target instead of the Service Level Target. The Extended Outage Target is calculated by dividing Scheduled Uptime less 2 hours and 54 minutes by Scheduled Uptime as follows:

(Scheduled Uptime – 2 hours 54 minutes)/ Scheduled Uptime.

(ii) **Number of Extended Outage Targets**: The number of Extended Outage Targets is calculated by rounding up to the nearest whole integer. For example, applying the standard of 1 production CICS region in every 10 would yield 1 Extended Outage Target for between 1 and 10 regions, 2 extended outages for between 11 and 20 regions, and 3 extended outages for between 21 and 30 regions.

(iii) **Compliance Calculation**: the entire SLA will be considered to have been achieved if each production CICS region achieves an Availability greater than or equal to the Service Level Target or to one of the allowed Extended Outage Targets

4.4 **Mainframe Availability – DB2.**

(a) Region Availability means the proportion of time a production DB2 region is in a functioning and accessible state.

(b) **Calculation**:

(i) **Extended Outage Targets**: one production DB2 region in every 10 is allowed an Extended Outage Target instead of the Service Level Target. The Extended Outage Target is calculated by dividing Scheduled Uptime less 2 hours and 54 minutes by Scheduled Uptime as follows:

(Scheduled Uptime – 2 hours 54 minutes)/ Scheduled Uptime.

(ii) **Number of Extended Outage Targets**: The number of Extended Outage Targets is calculated by rounding up to the nearest whole integer. For example, applying the standard of 1 production DB2 region in every 10 would yield 1 Extended Outage Target for between 1 and 10 regions, 2 extended outages for between 11 and 20 regions, and 3 extended outages for between 21 and 30 regions.

(iii) **Compliance Calculation**: the entire SLA will be considered to have been achieved if each production DB2 region achieves an Availability greater than or equal to the Service Level Target or to one of the allowed Extended Outage Targets

4.5 **Mainframe Availability – IMS.**

(a) Region Availability means the proportion of time a production IMS region is in a functioning and accessible state.

(b) **Calculation**:

(i) **Extended Outage Targets**: one production IMS region in every 10 is allowed an Extended Outage Target instead of the Service Level Target. The Extended Outage Target is calculated by dividing Scheduled Uptime less 2 hours and 54 minutes by Scheduled Uptime as follows:

(Scheduled Uptime – 2 hours 54 minutes)/ Scheduled Uptime.

(ii) **Number of Extended Outage Targets**: The number of Extended Outage Targets is calculated by rounding up to the nearest whole integer. For example, applying the standard of 1 production IMS region in every 10 would yield 1 Extended Outage Target for between 1 and 10 regions, 2 extended outages for between 11 and 20 regions, and 3 extended outages for between 21 and 30 regions.

(iii) **Compliance Calculation**: the entire SLA will be considered to have been achieved if each production IMS region achieves an Availability greater than or equal to the Service Level Target or to one of the allowed Extended Outage Targets

4.6 **Mainframe Availability – MQ.**

(a) Region Availability means the proportion of time a production MQ region is in a functioning and accessible state.

(b) **Calculation**:

(i) **Extended Outage Targets**: one production MQ region in every 10 is allowed an Extended Outage Target instead of the Service Level Target. The Extended Outage Target is calculated by dividing Scheduled Uptime less 2 hours and 54 minutes by Scheduled Uptime as follows:

(Scheduled Uptime – 2 hours 54 minutes)/ Scheduled Uptime.

(ii) **Number of Extended Outage Targets**: The number of Extended Outage Targets is calculated by rounding up to the nearest whole integer. For example, applying the standard of 1 production MQ region in every 10 would yield 1 Extended Outage Target for between 1 and 10 regions, 2 extended outages for between 11 and 20 regions, and 3 extended outages for between 21 and 30 regions.

(iii) **Compliance Calculation**: the entire SLA will be considered to have been achieved if each production MQ region achieves an Availability greater than or equal to the Service Level Target or to one of the allowed Extended Outage Targets.

4.7 **IMS Class 2 Performance.**

(a) **Transaction Response Time** means the time it takes an IMS production region to process a transaction but does not include the time to deliver the transaction to or from the IMS production region.

(b) **Compliance Calculation**: For each Measurement Window, compliance shall be measured by calculating the percentage of IMS Class 2 transactions completing in 3 seconds divided by total number IMS Class 2 transactions submitted, with the result expressed as a percentage and then comparing this percentage to the Service Level Target for this SLA. The SLA is considered achieved if the percentage if greater than or equal to the Service Level Target.

(c) Compliance Calculation is an aggregated of all Class 2 transactions by group. Class 2, 12, 22, 32, 42 are all Class 2 transactions but each group is specific to individual Clients .

(d) A Class 2 transaction has the following attributes: Is limited to 1.0124 CPU seconds Is limited to 25 DLI calls per scheduling Is limited to 12 physical I/Os.

4.8 **Batch Class 7 Performance.**

(a) Batch performance means that a submitted batch job read into the system, queued for processing and processes.

(b) **Compliance Calculation**: For each Measurement Window, compliance shall be measured by calculating the percentage of Class 7 batch jobs with a Job Turnaround Time less than or equal to the Turnaround Target divided by total number Class 7 batch jobs submitted, with the result expressed as a percentage, and then comparing this percentage to the Service Level Target for this SLA. The SLA is considered achieved if the percentage if greater than or equal to the Service Level Target. Where:

(i) **Job Turnaround Time** is the sum of: (1) the queue time between the last card image read and the start of the job execution, plus (2) the job elapse time between the start of job execution and job termination;

(ii) **Turnaround Target** is the sum of 30 minutes queue time plus execution target time, where execution target time equals the sum of (Task Control Block (TCB) time * 8) plus ((Service Request Block (SRB) time + Integrated Cryptographic Service Facility (ICSF) time)* 240) plus (number of tape mounts * 120).

SERVICE LEVEL OBJECTIVES (SLO)

This Section sets forth qualitative descriptions of the Service Level Objectives (SLOs). The numerical Service Level Targets, Measurement Windows, Support Hours and commencement of obligations associated with such SLOs are set forth in Appendix 11–A (*Service Level Measurements*).

5. PERFORMANCE CATEGORY – MIDRANGE

5.1 Tier 2 – General Business – Aged Infrastructure Availability.

This Tier is for single servers (i.e. non-clustered) in a data centre that are more than five (5) years old. Servers in this Tier are physical servers.

Notes:

(a) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLO.

(b) Availability Percentage Calculation: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (Midrange Availability Calculation).

(c) Compliance Calculation: The Availability will be calculated on each Server in this Tier separately. The SLO will be achieved if all Servers have an Availability greater than or equal to the Service Level Target.

5.2 Tier 3 - Remote Server Availability.

Servers in this Tier are physical servers located in the Regional Network Centres and Remote Sites (as defined in the Server Management Services SOW).

Notes:

(a) Application maintenance, recovery, performance and general availability responsibilities reside with the Province. Therefore the time or effort to recover Application services is not calculated in this SLO.

(b) Due to the varying distances that a technician may have to travel to service the Server and related equipment, all required travel time, including multiple trips if required, will be omitted from the Service Level calculation, provided that the Service Provider complies with the provisions of Appendix D (Supported Customer Locations) of the On Site Services SOW.

(c) For this Service Level the Remote Sites will be configured as described in the Data Center SOW.

(d) **Availability Percentage Calculation**: Please see the "Midrange Availability Calculation Summary" summary under Section 1 (Midrange Availability Calculation).

(e) **Compliance Calculation**: The Availability will be calculated by aggregating the results of all Servers in this Tier category together to arrive at an average (e.g. the sum of all Actual Uptimes divided by the sum of all Scheduled Uptimes expressed as a percentage). The SLO will be achieved if the average of all servers have an Availability greater than or equal to the Service Level Target.

5.3 **Midrange Provisioning - Standard Physical Server (within 4 weeks).**

A "Standard Physical Server" is a server defined in the approved Service Catalogue

Notes:

(a) Time spent during the process waiting on the Province task is not included in this Service Level (such as ICTR form approval).

(b) **Calculation Notes**: The time to provision a server for this calculation starts from the point in time that financial approval for the provisioning of a Standard Physical Server for is received by the Service Provider through the Province Ordering System. The time to provision a server ends when the server is available to Province for its application/use. The Province may have to perform activities (such as install Applications, load data), these activities are not part of the time to provision a server.

(c) **Compliance Calculation**: The compliance calculation shall be the number of Standard Physical Server requests provisioned within the Service Level Target divided by the total number of Standard Physical Server provisioning requests whose provisioning timeframe ends within the Measurement Window.

5.4 **Midrange Provisioning - Custom Physical Server (within 8 weeks).**

A "Custom Physical Server" is a server that is not defined in the approved Service Catalogue.

Notes:

(a) Time spent during the process waiting on the Province task is not included in this Service Level (such as ICTR form approval).

(b) **Calculation Notes**: The time to provision a server for this calculation starts from the point in time that financial approval for the provisioning of an additional Custom Physical Server is received by the Service Provider through the Province Ordering System. The time to provision a server ends when the server is available to Province for its application/use. The Province may have to perform activities (such as install Applications, load data), these activities are not part of the time to provision a server.

(c) **Compliance Calculation**: For a given Measurement Window, the compliance calculation shall be the number of Custom Physical Server requests provisioned within the Service Level Target divided by the total number of Custom Physical Server provisioning requests whose provisioning timeframe ends within the Measurement Window.

5.5 **Midrange Provisioning - Standard Virtual Server (within 3 days).**

A Standard Virtual Server is a virtual server defined in the approved Service Catalogue.

Notes:

(a) Other than in an STMS Data Centre, this SLO will be suspended where a Province does not provide the Service Provider with the necessary server configuration information (such as server name, IP address, Operating System particulars) either as part of the virtual server request or within 4 business hours of a request for such information from the Service Provider, in which case, the SLO shall be suspended for any excess delay beyond such 4 hour period.

(b) Time spent during the process waiting on the Province task is not included in this Service Level (such as ICTR form approval).

(c) Procurement activities are from 8:00 AM to 5:00 PM on Business Days.

(d) Implementation services may be performed outside of 8:00 AM to 5:00 PM on Business Days.

(e) **Calculation Notes**: The time to provision a server for this calculation starts from the point in time that financial approval for the provisioning of an additional Standard Virtual Server is received by the Service Provider through the Province Ordering System. The time to provision a server ends when the server is available to Province for its application/use. The Province may have to perform activities (such as install Applications, load data), these activities are not part of the time to provision a server.

(f) **Compliance Calculation**: For a given Measurement Window, the compliance calculation shall be the number of Standard Virtual Server requests provisioned within the Service Level Target divided by the total number of Standard Virtual Server provisioning requests whose provisioning timeframe ends within the Measurement Window.

6. **PERFORMANCE CATEGORY – STORAGE**

6.1 **Time to Provision Storage.**

(a) The time to complete an allocation is measured from the point in time that financial approval for the provisioning of a storage device is received by the Service Provider through the Province Ordering System until the point that the

storage is provisioned and ready for use by the Province. For the Significant and the Major Allocation Types, prior to providing an approved request to the Service Provider, Province will confirm with Service Provider that the hardware resources are available to provide the allocation within the Provisioning Timeframe.

(b) "**Provisioning Timeframe**" shall be set by the type of request as follows:

Allocation Type	Allocation Size	Provisioning Timeframe
Level 1 (Major)	3TB – 10TB	15 Business Days
Level 2 (Significant)	(300GB - 3TB)	5 Business Days
Level 3 (Minor)	1 Business day (300GB)	1 Business Day
Level 4 (Emergency)	4-8 hours (300GB)	8 hours

(c) **Compliance Calculation:** For a given Measurement Window, the compliance calculation shall be the total number of storage allocation requests completed within the Provisioning Timeframe, divided by the Total number of storage allocation requests whose provisioning timeframe ends in the Measurement Window, with the result expressed as a percentage and then comparing this percentage to the Service Level Target for this SLO. The SLO is considered achieved if the percentage greater than or equal to the Service Level Target.

7. PERFORMANCE CATEGORY – CROSS FUNCTIONAL

7.1 Response to Priority 3 Incident within target.

(a) **Response** means the acknowledgement by Service Provider of a Priority 3 Incident assigned by the Province Service Desk. The Service Provider acknowledgement shall be the earlier of:

(i) a verbal acknowledgement recorded by the Province Service Desk; or

(ii) the time that an incident is created in ITIMS in response to notifications about a previously auto-generated and assigned incident; or

(iii) the time that the Service Provider assigned the Incident to be worked as recorded on the bridged incident record.

(b) **Target** means: two (2) hours during the hours of 8 AM to 5 PM on Business Days.

(c) **Compliance Calculation**: For any Measurement Window, compliance shall be calculated as the number of Priority 3 Incidents allocated to Service Provider by the Province Service Desk that are responded to within Target, divided by the number of Priority 3 Incidents allocated to the Service Provider, with the result expressed as a percentage to two decimal places, and comparing this percentage to the Service Level Target for this SLO.

(d) **Exclusion**: For Priority 3 incidents, communication of the Priority 3 assignment from the Province Service Desk to the Service Provider is expected to be completed within a period of time that is equal to 10% of the Target. Incidents where communication is interrupted or delayed by the Province Service Desk will be excluded from compliance calculations.

7.2 **Response to Priority 4 Incident within target.**

(a) **Response** means the acknowledgement by Service Provider of a Priority 4 Incident assigned by the Province Service Desk. The Service Provider acknowledgement shall be the earlier of:

(i) a verbal acknowledgement recorded by the Province Service Desk; or

(ii) the time that an incident is created in ITIMS in response to notifications about a previously auto-generated and assigned incident; or

(iii) the time that the Service Provider assigned the Incident to be worked as recorded on the bridged incident record

(b) **Target** means: Two (2) hours during Regular the hours of 8 AM to 5 PM on Business Days

(c) **Compliance Calculation**: For any Measurement Window, compliance shall be calculated as the number of Priority 4 Incidents allocated to Service Provider by the Province Service Desk that are responded to within Target, divided by the number of Priority 4 Incidents allocated to the Service Provider, with the result expressed as a percentage to two decimal places, and comparing this percentage to the Service Level Target for this SLO.

(d) **Exclusion**: For Priority 4 incidents, communication of the Priority 4 assignment from the Province Service Desk to the Service Provider is expected to be completed within a period of time that is equal to 10% of the Target. Incidents where communication is interrupted or delayed by the Province Service Desk will be excluded from compliance calculations.

7.3 **Update to Priority 1 Incident within Target.**

(a) **Update** means the status update by Service Provider of a Priority 1 Incident during the period from when an Incident is allocated to the Service Provider until the Incident is resolved.

(b) **Target** means:

(i) sixty (60) minutes during regular the hours of 8 AM to 5 PM on Business Days

(ii) Sixty (60) minutes during the hours of 5 PM to 8 AM during Support Hours.

(c) **Compliance Calculation**: For any Measurement Window, compliance shall be calculated as the number of Priority 1 Incidents allocated to Service Provider that have an Update within Target, divided by the number of Priority 1 Incidents allocated to the Service Provider, with the result expressed as a percentage to two decimal places, and comparing this percentage to the Service Level Target for this SLO. The SLO is considered achieved if the percentage if greater than or equal to the Service Level Target.

7.4 **Update to Priority 2 Incident within Target.**

(a) **Update** means the status update by Service Provider of a Priority 2 Incident during the period from when an Incident is allocated to the Service Provider until the Incident is resolved.

(b) **Target** means:

(i) ninety (90) minutes during regular the hours of 8 AM to 5 PM on Business Days

(ii) Ninety (90) minutes during the hours of 5 PM to 8 AM during Support Hours.

(c) **Compliance Calculation**: For any Measurement Window, compliance shall be calculated as the number of Priority 2 Incidents allocated to Service Provider that have an Update within Target, divided by the number of Priority 2 Incidents allocated to the Service Provider, with the result expressed as a percentage to two decimal places, and comparing this percentage to the Service Level Target for this SLO. The SLO is considered achieved if the ratio if greater than or equal to the Service Level Target.

7.5 **Change Management - Successful Changes.**

(a) **Successful Change** means an approved change, through the Change Management System, implemented without negative impact to the Client in the agreed timeframe. It excludes Emergency Changes.

(b) **Compliance Calculation**: For any Measurement Window, compliance shall be calculated as the number of Successful Changes divided by the total number of changes scheduled to be completed during the Measurement Window, with the result expressed as a percentage, and comparing this percentage to the Service Level Target for this SLO. The SLO is considered achieved if the percentage is greater than or equal to the Service Level Target.

8. PERFORMANCE CATEGORY – MAINFRAME

8.1 CICS Transaction Speed measured by customer application summary set completion.

(a) Transaction speed or transaction response time means the time it takes a CICS region to process a transaction but does not include the time to deliver the transaction to or from the CICS region.

(b) **Compliance Calculation**: as calculated by vendor tools using the Service Level Target for this SLO.

8.2 IMS Transaction Speed per defined IMS transaction classes.

(a) Transaction Speed or transaction response time means the time it takes an IMS region to process a transaction but does not include the time to deliver the transaction to or from the IMS region.

(b) **Compliance Calculation**: as calculated by vendor tools using the Service Level Target for this SLO.

8.3 TSO Transaction Speed per defined TSO transaction classes.

(a) Transaction Speed or transaction response time means the time it takes an TSO to process a transaction but does not include the time to deliver the transaction to or from the LPAR.

(b) **Compliance Calculation**: as calculated by vendor tools.

8.4 Batch Completion Rates per defined batch job classes.

(a) Batch completion rates is the success rates of completing the processing of all jobs by class by a given time of day.

(b) **Compliance Calculation**: as calculated by vendor tools using the Service Level Target for this SSLO.

9. PERFORMANCE CATEGORY – SERVICE DESK

After Hours Service Desk Hours of Operation

The Hours of Operation for the Customer Service Centre ("**CSC**") After Hours Service Desk hours are:

- Monday 7:00 PM to Tuesday 7:00 AM
- Tuesday 7:00 PM to Wednesday 7:00 AM
- Wednesday 7:00 PM to Thursday 7:00 AM
- Thursday 7:00 PM to Friday 7:00 AM

- Friday 7:00 PM to Monday 7:00 AM
- Statutory holidays, in effect as of the Hand-Over Date, applicable to the British Columbia Public Service
- CSC Monthly Staff Meetings (1 hour per calendar month)

9.1 **Service Desk Speed to Answer.**

(a) **Speed to Answer** shall mean the time an end user has to wait for a live Service Desk agent to answer a telephone inquiry.

(b) **Data Capture**: Speed to answer is monitored via the applicable Automated Call Distribution (ACD) system.

(c) **Compliance Calculation**: For any Measurement Window, during the Hours of Operation, the total number of calls answered by a live Service Desk agent within 60 seconds after a request for a live Service Desk agent is made through the automated call distribution system during the CSC Hours of Operation divided by the total number of calls where a request for a live Service Desk agent is made via the automated call distribution system during the CSC Hours of Operation, with the result expressed a percentage and comparing this percentage to the Service Level Target for this SLO. The SLO is considered achieved if the percentage if greater than or equal to the Service Level Target.

9.2 **Service Desk Incident Creation Within Target.**

(a) **Incident Creation** within Target shall mean the time an Incident is created within Incident Management and dispatched to Second Level support.

(b) **Target** shall mean 8 minutes with the exception of B.C. Ambulance. All B.C. Ambulance contacts will be dispatched within 5 minutes.

(c) **Data Capture**: Time of dispatch is captured from the Province Incident Management System.

(d) **Compliance Calculation**: The total number of Incidents created within target within the Measurement Window, during the CSC Hours of Operation, divided by the total number of incidents during the Measurement Window, with the result expressed as a percentage, and comparing this percentage to the Service Level Target for this SLO. The SLO is considered achieved if the percentage if greater than or equal to the SLO.

APPENDIX 11-C

DATA CENTER SERVICE LEVELS

1. **Definitions.** For purposes of this Appendix, the following words shall have the following meanings:

"**7/24 Basis**" means seven days/week, 24 hours/day.

"**Business Hours**" means Monday through Friday between the hours of 6 AM and 8 PM, local data centre time.

"**Controllable Event**" shall have the meaning assigned to such term in Section 10 below.

"**Cooling Availability**" means cooling capacity to the Customer Environment at the STMS Data Centres, where the cooling capacity has been provisioned to effectively cool Customer Provided Equipment that consumes an average of 100 watts per square foot.

"**Cooling Outage**" means the failure of any cooling systems resulting in a failure to provide Cooling Availability within the Customer Environment, except a failure of any cooling system as a result of the improper distribution, installation or operation of Customer Provided Equipment.

"**Customer Environment**" has the meaning given to it in the Data Centre Services SOW.

"**Customer Provided Equipment**" has the meaning given to it in the Data Centre Services SOW.

"**Emergency Escalation List**" means a contact list of representatives of the Customer identified in the STMS Data Centre Control Panel.

"**Emergency Maintenance**" means maintenance that must be performed by the Service Provider, because of an imminent risk to the operation of the STMS Data Centre, prior to the next Standard Maintenance Window where there is insufficient time for the Service Provider to include maintenance in a Non-Standard Maintenance Window.

"**Interruption**" means a situation where the Customer has encountered a apparent interruption of service that may be as a result of services provided by the Service Provider.

"**Major Cooling Outage**" means a complete failure to provide Cooling Availability within the Customer Environment.

"**Major Power Loss**" means the complete failure to provide Power Availability within the Customer Environment.

"**Non-Standard Maintenance Windows**" means non-standard maintenance windows which may be scheduled by the Service Provider, in its sole discretion, Monday through Friday during Business Hours or outside of Business Hours.

"**Potential Deficiency**" means a situation where the Customer is encountering performance issues within its Customer Environment that may be as a result of services provided by the Service Provider.

"**Power Loss**" means the failure to provide Power Availability of any duration to one or more racks or cabinets contained within the Customer Environment, excluding a power loss caused by Customer Provided Equipment failure or Customer power circuits overloading.

"**Power Availability**" means continuous power to at least one of the Customer's power circuits for each rack or cabinet (as applicable) contained within the Customer Environment in a STMS Data Centre(s), where power has been provisioned to the Customer's power circuits within the Customer Environment from independent power sources.

"**Standard Maintenance Windows**" means standard maintenance windows scheduled between 2 AM and 5AM local data centre time on Sundays and Thursdays.

2. **Purpose**. The purpose of this Appendix is to describe the Service Levels applicable to the Services provided by the Service Provider to the Customer. The Service Provider is required to meet or exceed the Service Levels, failing which, the Service Provider shall be subject to DC Service Level Credits (as defined in Schedule 12 (*Service Level Failures*) of the Agreement. The Service Provider's failure to meet any Service Level shall result in the Customer being entitled to apply (or set-off) the amount of the Service Level Credit in accordance with the terms of this Schedule against the monthly VA Fees owing by the Customer to the Service Provider under the Agreement.

3. **Service Levels Agreements and DC Service Level Credits**. The Service Provider agrees to meet or exceed the following Service Levels for the Services set out in the Agreement and shall be liable for any failure in such Service Level and for the DC Service Level Credits set forth in the table below.

	Service Level	Metric	Scope	Process	DC Service Level Credit
1.	Power Availability at the STMS Data Centres.	100% Power Availability on a 7/24 Basis.	The Service Provider will provide Power Availability to the Customer Environment.	In the event of a Power Loss, the Service Provider or Customer shall trigger the opening of a trouble ticket, attributable to the power loss event. Within 45 minutes of the opening of a Power Availability trouble ticket, the Service Provider will determine the cause of the power loss (whether the power loss is caused by Customer Provided Equipment or otherwise) and notify the Customer of such cause. On a monthly basis the Service Provider will provide the Customer with a report of any and all Power Loss during the month including the details of such Power Loss (including, without limitation time of Power Loss, duration of Power Loss and such other relevant information). The length of a Power Loss is calculated by the Service Provider and will commence upon the earlier of: (a) the opening of the trouble ticket by the Service Provider or the Customer (see Section 5 below) and; (b) the time that the STMS Data Centre Control Centre first records the Power Loss (through	In the event of a Power Loss, for each hour (or any partial hour) of a Power Loss, a DC Service Level Credit equivalent to $1/30^{th}$ of the Customer's monthly VA Fees for that portion of the Customer's Capacity Reservation affected by the Power Loss, which amount will be set-off by the Service Provider against the VA Fees payable by the Customer to the Service Provider, and reflected in the Service Provider's next monthly invoice to the Customer. In the event that there are multiple incidents of power loss within a single one-hour period, such intermittent power losses shall constitute a single Power Loss event for the purposes of the DC Service Level Credit.

	Service Level	Metric	Scope	Process	DC Service Level Credit
				the automated monitoring system records, trouble tickets opened by the Customer or other affected customers, or otherwise); and ending when the Service Provider makes its initial attempt to notify the Customer of restoration of 100% Power Availability by calling the first name on the Customer's Emergency Escalation List.	
2.	Cooling at the STMS Data Centre(s).	100% Cooling Availability.	The Service Provider will provide Cooling Availability to the Customer Environment.	In the event of a Cooling Outage, the Service Provider or Customer shall trigger the opening of a trouble ticket, attributable to the cooling outage event. Within 45 minutes of the opening of a Cooling Availability trouble ticket, the Service Provider will determine the cause of the cooling failure (whether the cooling failure is caused by the Customer Provided Equipment or otherwise) and notify the Customer of such cause. On a monthly basis the Service Provider will provide the Customer with a report of any and all Cooling Outages during the month including the details of such Cooling Outage (including, without limitation, time of Cooling Outage,	In the event of a Cooling Outage, for each hour (or any partial hour) of a Cooling Outage, a DC Service Level Credit equivalent to $1/30^{th}$ of the Customer's monthly VA Fees for that portion of the Customer's Capacity Reservation affected by the Cooling Outage, which amount will be set-off by the Service Provider against the VA Fees payable by the Customer to the Service Provider, and reflected in the Service Provider's next monthly invoice to the Customer.

	Service Level	Metric	Scope	Process	DC Service Level Credit
				duration of Cooling Outage and such other relevant information). The length of a Cooling Outage is calculated by the Service Provider and will commence upon the earlier of: (a) the opening of the trouble ticket by the Service Provider or the Customer (see Section 5 below) and; (b) the time that the STMS Data Centre Control Centre first records the Cooling Outages (through the automated monitoring system records, trouble tickets opened by the Customer or other affected customers, or otherwise); and ending when the Service Provider makes its initial attempt to notify the Customer of restoration of 100% Cooling Availability, by calling the first contact on the Customer's Emergency Escalation List.	
3.	STMS Data Centre Control Centre ("**CC**").	STMS Data Centre CC will be in continuous operation.	The Service Provider will maintain the STMS Data Centre CC so that it continuously operates, on a 7/24 Basis, and monitor various STMS Data Centre Services in order to promptly detect any Potential Deficiencies or	An STMS Data Centre CC must respond to any CC Notification confirming receipt either by telephone or electronic mail within 20 minutes for telephonic notices, and 60 minutes for e-mail notices, following delivery of the Customer's CC Notification.	Each failure to respond within the time periods specified for a Customer CC Notification will entitle the Customer to a DC Service Level Credit equivalent to $1/30^{th}$ of the Customer's monthly VA Fees for the affected Service, which amount will be set-off by the Service Provider against the VA Fees payable by the Customer to the Service Provider, and reflected in the

	Service Level	Metric	Scope	Process	DC Service Level Credit
			Interruptions in the Data Centre Services and initiate corrective action as appropriate. In addition, the STMS Data Centre CC continuously accepts, reviews and responds to Customer notifications (see Section 5 below) of Potential Deficiencies or Interruptions (a **"CC Notification"**).		Service Provider's next monthly invoice to the Customer.

4. **Maintenance Windows.** The STMS Data Centres are designed to operate on a continuous basis; however, the Service Provider requires the ability to perform maintenance on the STMS Data Centre Systems, from time to time, during the Term of the Agreement.

(a) **Planned Maintenance**: In order to allow the Service Provider and the Customer to more effectively plan their operational requirements in advance, this Section 4 describes the times during which the Service Provider may perform planned maintenance ("Planned Maintenance") as described below, including a mechanism by which the Customer will be notified in advance of maintenance that may impact one or more Services. Planned Maintenance may be performed by the Service Provider either during a Standard Maintenance Window or a Non-Standard Maintenance Window provided that:

(i) ***Notice of Service Impacting Maintenance***: The Service Provider will provide the Customer with prior notice describing the specific service potentially impacted and the expected nature and extent of the reduction or other effect on the applicable service (a "**Potential Service Impact Notice**") if the Service Provider intends to perform Planned Maintenance that may impact one or more services ("**Service Impacting Maintenance**") during either a Standard Maintenance Window or a Non-Standard Maintenance Window;

(ii) ***Standard Maintenance Windows***: The Service Provider will, where reasonably possible, perform Service Impacting Maintenance during Standard Maintenance Windows.

(iii) ***Non-Standard Maintenance Windows***:

(A) ***During Non-Business Hours Service***: The Service Provider may schedule a Non-Standard Maintenance Window to perform Planned Maintenance outside of Business Hours by providing the Customer with a Potential Service Impact Notice 48 hours prior to the Service Provider commencing performance of Service Impacting Maintenance;

(B) ***During Business Hours***: The Service Provider may request a Non-Standard Maintenance Window to perform Planned Maintenance during Business Hours by giving five (5) Business Days prior Potential Service Impact Notice to the Customer, in which case, the Customer has the right to object to such Service Impacting Maintenance by providing the Service Provider with notice within two (2) Business Days of the date of the Potential Service Impact Notice, including reasons for the objection to enable the Service Provider to assess an alternate time to perform such Planned Maintenance. Upon receipt of such objection, the Service Provider shall reschedule such proposed Non-Standard Maintenance Window. If the Customer does not provide an objection to the

Service Provider within the two (2) Business Days, the Service Provider shall have the right to perform such Planned Maintenance during the Non-Standard Maintenance Window scheduled by the Service Provider in accordance with its original notice.

(iv) ***DC Service Level Credits During Standard Maintenance Windows and Non-Standard Maintenance Windows***: In the event of a Service Level failure occurring during a Standard Maintenance Window or a Non-Standard Maintenance Window where the Service Provider:

(A) has provided the Customer with a Potential Service Impact Notice, then the Customer shall not be eligible for DC Service Level Credits for Service Level failures occurring during such Standard Maintenance Window or Non-Standard Maintenance Window; and

(B) has not provided the Customer with a Potential Service Impact Notice, then the Customer shall be eligible for DC Service Level Credits in accordance with the terms of this Appendix 11-C for Service Level failures occurring during such Standard Maintenance Window or Non-Standard Maintenance Window.

(b) **Emergency Maintenance**:

(i) ***Notification of Customer***: If the Service Provider performs Emergency Maintenance, it will, to the extent reasonably possible in the circumstances, notify the Customer prior to performing such Emergency Maintenance.

(ii) ***DC Service Level Credits During Emergency Maintenance***: Where any Service Level failure arises as a result of Emergency Maintenance required to be performed due to circumstances outside of the Service Provider's reasonable control, the Customer shall not be entitled to DC Service Level Credits. If, however, the Emergency Maintenance was required as a result of circumstances which could have reasonably been anticipated by the Service Provider and avoided through the scheduling of Planned Maintenance, then the Customer will be eligible for DC Service Level Credits in respect of any such Service Level failure resulting from such Emergency Maintenance.

(c) ***Limits on Relief of DC Service Level Credits***: Notwithstanding the provisions of Section 4(a)(iv)(A) or 4(b)(ii), the Service Provider shall pay the DC Service Level Credits for any Service Level failures in a given consecutive 12-month period that follow: (i) three (3) Service Level failures in such consecutive 12-month period; or (ii) one Service Level failure per 100,000 VA's of Capacity Reservation or Adjusted Capacity Reservation, as the case may be, in such consecutive 12 month period, whichever is greater.

5. **Notification by Customer**. In the event the Customer believes that: (a) a failure has occurred in connection with or relating to the Customer Environment; or (b) Potential Deficiencies or Interruptions may occur, the Customer should contact the Service Provider (in accordance with the method of contact recommended and communicated to the Customer by the Service Provider, in writing, as contemplated under the Data Centre Service SOW) and request that a trouble ticket specific to the event be opened. Once a ticket has been opened (either at the request of the Customer, another customer or through the Service Provider automated monitoring system), the Service Provider will promptly initiate diagnostic testing and trouble isolation to determine the nature of the service quality or availability event. If the trouble is diagnosed as one that may be within the scope of coverage, responsibility and management of the trouble ticket will be assumed by the Service Provider. The Service Provider has no obligation to issue a DC Service Level Credit where no trouble ticket has been opened by either the Service Provider or the Customer and further has no obligation to issue a DC Service Level Credit where the Customer has not formally requested a DC Service Level Credit within 30 days of an eligible event if the Customer believes a DC Service Level Credit is due.

6. **Single Incident/Multiple DC Service Level Credits; Service Level Requirements**. If a single incident results in the failure of the Service Provider to meet more than one Service Level, the Customer shall have the right to select any one of such multiple Service Levels for which it will be entitled to receive a DC Service Level Credit. (The Customer shall not be entitled to a DC Service Level Credit for each missed Service Level.), Furthermore, for purposes of clarification, any and all references in Section 8.9 (*Service Level Failures*) of the Agreement to the failure of the Service Provider to meet a Service Level Agreement, or such similar references, shall mean the Service Provider's complete failure to provide or otherwise perform the Service Level metric to which the Service Level Agreement applies.

7. **Maximum DC Service Level Credit**. The aggregate amount of DC Service Level Credits payable by the Service Provider to the Customer under this Appendix 11-C (Data Center Service Levels) in respect of any one month shall not exceed the sum of (i) the Customer's monthly VA Fees for such month plus (ii) an amount equal to any DC Service Level Credits which may apply under Section 10 and are attributable to Controllable Events which occur in such month.

8. **Conduct Permitting Relief from Service Levels**. The Service Provider shall not be considered to have failed to meet a Service Level to the extent that the Customer's acts, omissions or instructions to Service Provider cause the failure.

9. **Steps for Relief**. To obtain relief from any Service Level in the case of the events described in Section 8:

(a) the Service Provider must provide specific notification to the Customer that describes to the Customer in writing the specific Service Level impacted and the expected nature and extent of the reduction or other effect on the applicable Service Level, including any significant additional unanticipated costs; and

(b) the Service Provider must in each instance have used all commercially reasonable efforts to perform the affected Service or resolve the incident or problem in accordance with the applicable Service Levels despite such events.

10. **Service Level Termination Event.** Subject to any conduct permitting relief from Service Levels or other exceptions to service delivery as set forth in this Appendix 11-C or the Agreement, a Service Level event (an "**Event**") will be considered to have occurred upon any of the following:

(a) a Major Power Loss for more than 10 minutes; or

(b) a Major Cooling Outage for more than 10 minutes; or

(c) at least three hours or more of any combination of Power Loss or Cooling Outage within any consecutive three month period, where any Power Loss contributing to such three hour period affected at least ten percent (10%) of the Capacity Reservation or Adjusted Capacity Reservation, as the case may be, in the Customer Environment and any Cooling Outage contributing to such three hour period affected at least twenty percent (20%) of the Capacity Reservation or Adjusted Capacity Reservation, as the case may be, in the Customer Environment;

provided that, notwithstanding the length or quantity of such failures, no combination of failures of the Service Provider to attain a Service Level in any consecutive twenty four (24) hour period will be considered as more than a single Event.

Upon the occurrence of an Event, the Service Provider will promptly carry out a root cause analysis for the purpose of identifying the cause of such Event. If the Event is determined after a root cause analysis to be due to events or circumstances within the reasonable control of the Service Provider acting as a prudent operator of a data center facility which is similar or substantially similar to the STMS Data Centre, having regard to the Service Provider's responsibilities under the Agreement (a "**Controllable Event**"), then the Customer shall have the following remedies, in addition to the DC Service Level Credits set forth in Section 3 above:

(i) on the first occurrence of a Controllable Event within any given consecutive 12 month period, a DC Service Level Credit in an amount equal to the then current monthly VA Fees, which amount will be set-off by the Service Provider against the VA Fees payable by the Customer to the Service Provider and reflected in the Service Provider's next monthly invoices to the Customer;

(ii) on the second occurrence of a Controllable Event within any given consecutive 12 month period, a DC Service Level Credit in an amount equal to two (2) times the then current monthly VA Fees, which amount will be set-off by the Service Provider against the VA Fees payable by the Customer to the Service Provider and reflected in the Service Provider's next monthly invoices to the Customer; and

(iii) on the third or greater occurrence of a Controllable Event within any given consecutive 12 month period, the Customer may either:

(A) elect to receive a DC Service Level Credit in an amount equal to four (4) times the then current monthly VA Fees , which amount will be set-off by the Service Provider against the VA Fees payable by the Customer to the Service Provider and reflected in the Service Provider's next monthly invoices to the Customer; or

(B) declare the Controllable Event to be a Service Level Termination Event by providing written notice thereof to the Service Provider no later than thirty (30) days following such third or greater Controllable Event, and such Service Level Termination Event shall constitute a Material Breach by the Service Provider under Section 28.1 of the Agreement; provided, however, that if the Customer decides to terminate the Agreement as a result of a Service Level Termination Event, the Customer must include written notice of termination with its declaration of a Service Level Termination Event.

APPENDIX 11-D

REPORTS

#	Name			Mar-2010	Feb-2010	Jan-2010	Dec-2009	Nov-2009	Oct-2009	Sep-2009	Aug-2009	Jul-2009	Jun-2009	May-2009	Apr-2009
	Performance Category - Midrange	Measurement Window	Service Level Target	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual
1.1	Tier 1 - Business Priority - Geographically Distributed Cluster with sychronous data replication	7x24	99.999%	100.000%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
1.2	Tier 1 - Business Priority - Geographically Distributed Cluster with asychronous data replication	7x24													
1.3	Tier 1 - Business Priority - Clustered in a single location	7x24													
	... (SAMPLE FORMAT)														
	Performance Category - Storage	Measurement Window	Service Level Target	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual	Actual
2.1	Tier 1 - Mission Critical Storage Availability	7x24	99.999%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	... (SAMPLE FORMAT)														

Number	Date	SLA #	Name	Target	Particulars of Failure (month)	Corrective Action Plan	Corrective Action Plan Target Date	Plan Status	Comments
yyyy-cc	yyyy-mm	1.1	Tier 1 - Business Priority - Geographically Distributed Cluster with sychronous data replication	Expected	Availability of XXXX cluster below target due to impact of incident #	Corrective action plan #xxxxx-xxx			

SCHEDULE 12

SERVICE LEVEL FAILURES

(Section 8.9)

1. **Purpose.** Further to Section 8.9 (*Service Level Failures*) of the Agreement, the purpose of this Schedule is to describe the consequences of failure of the Service Provider to achieve the Service Levels.

2. **Definitions.** Where used in this Schedule, the following words will have the meanings set forth below, and any other words defined in this Schedule will have the meanings so given to them:

(a) "**Data Center SLAs**" means those Service Levels designated as such in Appendix 11-C (*Data Center Service Levels*);

(b) "**Managed Services SLAs**" means those Service Levels designated as such in Appendix 11-A (Service *Level. Measurements*);

(c) "**Monthly Fees**" means the total Fees invoiced by the Service Provider in any month for Services provided to the Province, excluding (a) Fees for Transformation Services, (b) Fees for the STMS Data Center Services; (c) annual Capital Payment, (d) Fees for projects (excluding credit bearing performance measures that can be established per project related requests submitted through the Change Order Process), (e) Fees for standard Time and Materials Services, (f) Taxes, (g) Pass Through Expenses, and (h) any other Out-of-Pocket Expenses that are reimbursable to the Service Provider by the Province in accordance with the Agreement; provided that for purposes of calculating the Maximum At Risk Amount based upon the 12.5% factor, the "Monthly Fees" will be the greater of the amount calculated according to the above definition and $3,500,000;

(d) "**SLA Failure**" means Service Provider's performance against a Service Level Agreement, as measured in accordance with the provisions of Appendix 11-A, has not achieved the stated level.

3. **Managed Services: Service Level Credits.** A Managed Services SLA Failure shall result in the Province being entitled to apply service level credits ("**Service Level Credits**") against the Monthly Fees owed by the Province to the Service Provider under this Agreement, commencing on the seventh (7^{th}) month following the Hand-Over Date, as follows:

(a) Service Level Credits may only be earned in the event of a failure by the Service Provider to achieve a Managed Services SLA;

(b) the monthly maximum Service Level Credits to which the Province shall be entitled shall not exceed the following:

(i) for the period commencing with the seventh (7^{th}) month and ending with the twelfth (12^{th}) month following the Hand-Over Date (the "**SLA Ramp-up Period**"), an amount equal to six and one-quarter percent (6.25%) of the Monthly Fee for the month in which such SLA Failure occurs; and

(ii) for any month after the SLA Ramp-up Period, twelve and one half percent (12½%) of the Monthly Fee for the month in which such SLA Failure occurs;

(the "**Maximum At Risk Amount**");

(c) the Province has assigned percentage points of multipliers ("**Weightings**") to the Managed Services SLAs as set out in Appendix 11-A (*Service Level Measurements*). The Province may change the Weightings attached to the Managed Services SLAs in accordance with **Schedule 13** *(Changes to Weightings)* of the Agreement, provided that:

(i) the aggregate Weightings attached to the Managed Services SLAs may not exceed two hundred and fifty percent (250%),

(ii) the Weighting attached to any one Managed Services SLA may not exceed twenty percent (20%), and

(iii) the Weighting attached to a Managed Services SLA may be zero percent (0%),

(d) commencing with the seventh (7^{th}) month following the Hand-Over Date, and for all Managed Services SLAs other than the Midrange Server SLA (defined in paragraph (e) below), if the Service Provider fails to achieve any Managed Services SLA in any given month, then subject to Section 7 (*Earnback Credits*) below, the Province shall earn a Service Level Credit in respect of such missed Managed Services SLA in an amount equal to the product of:

(i) the Weighting attached to the missed Managed Services SLA, and

(ii) the applicable Maximum At Risk Amount;

(e) commencing with the seventh (7^{th}) month following the Hand-Over Date, and for the Managed Services SLAs for the Tier 1 Midrange Servers (the "**Midrange Server SLA**"), if the Service Provider fails to achieve the Midrange Server SLA in any given month, then subject to Section 7 (*Earnback Credits*) below, the Province shall earn a Service Level Credit in respect of such missed Midrange Server SLA in an amount equal to the product of:

(i) the Weighting attached to the missed Midrange Server SLA;

(ii) the applicable Maximum At Risk Amount; and

(iii) the applicable Midrange Tier 1 Factor, as indicated in the Table below.

Number of Clusters in SLA	Midrange Tier 1 Factor
1 to 10 clusters	1.0
11 to 20 clusters	0.5
21-33 clusters	0.33
31 – 40 clusters	0.25

(f) if the Service Provider fails to achieve more than one Managed Services SLA in a given month, then the Province shall earn an aggregate amount equal to the sum of the Service Level Credits corresponding to such failed Managed Services SLAs; provided that the Province may not earn more than the applicable Maximum At Risk Amount in Service Level Credits in any one month.

4. **Data Center Service Level Credits.** The Service Provider's failure to achieve any Data Center SLAs shall result in the Province being entitled to apply service level credits ("**DC Service Level Credits**") as set forth in Appendix 11-C (*Data Center Service Levels*).

5. **Single Problem, Multiple Occurrences.** Upon the occurrence of a single Problem that causes a failure in multiple SLAs (including multiple Managed Services SLAs and/or Data Centre SLAs), the Province may only earn one (1) Service Level Credit in respect of one (and not all) of such affected SLAs (the "**Single Problem SLA**"), which Service Level Credit shall be selected by the Province in its sole discretion and for greater clarification, the Downtime caused by the occurrence of that Problem shall only be calculated against the Single Problem SLA for which the Province elects to receive a Service Level Credit, and not against the other SLAs affected by that same Problem.

6. **Performance Obligation.** Notwithstanding the foregoing, and for greater clarification, the Service Provider shall use commercially reasonable efforts to achieve all Service Levels, whether or not such Service Levels are subject to Service Level Credits.

7. **Earnback Credits.** The Service Provider shall be entitled to earn back credits (**"Earnback Credits"**) for each Managed Services SLA where the Service Provider achieves or exceeds that same Managed Services each month during a period of six (6) consecutive months (the "**Earnback Period**"). The Earnback Credits may be applied by the Service Provider to offset against Service Level Credits for that same Managed Services SLA as set out in this Section 10 (*Earnback Credits*) below. The Earnback Credits shall be subject to the following:

(a) if the Service Provider consistently achieves or exceeds the same Managed Services SLA in each month during the Earnback Period, then the Service Provider shall earn one Earnback Credit for that specific Managed Services SLA;

(b) if the Service Provider fails to achieve a Managed Services SLA in any month, then the Earnback Period for that Managed Services SLA shall be reset and shall start again; and

(c) the Service Provider may accumulate up to a maximum of one (1) Earnback Credit for each specific Managed Services SLA at any given time; provided that, upon reaching the maximum, the Service Provider shall not earn any further Earnback Credits for that Managed Services SLA until such time as the accumulated Earnback Credit is utilized by the Service Provider and applied against a Service Level Credit for such Managed Services SLA in accordance with this Section 10 (*Earnback Credits*).

If the Service Provider accumulates Earnback Credits for a particular Managed Services SLA, then notwithstanding that the Province may have earned a Service Level Credit in respect of that same Managed Services SLA failure in any given month, the Service Provider shall be released from the obligation to pay the Service Level Credit by setting off the Earnback Credit against the Service Level Credit for such Managed Services SLA.

8. **Global Credits.** As of the Effective Date, the Service Provider shall have three (3) banked Earnback Credits (the "**Global Credits**"), which Global Credits may be applied by the Service

Provider to offset Service Level Credits for the failure of any Managed Services SLA, provided that any unused Global Credits shall expire and be of no force or effect as of May 1, 2014.

9. **Monthly Reconciliation.** In conjunction with the monthly invoicing of the Fees to the Province (as specified in Schedule 23 (*Fees*) of the Agreement), the Parties shall make all necessary adjustments to the Service Level Credits as described in Section 10 (*Earnback Credits*), and any Service Level Credits remaining after such adjustment shall be set-off against the Fees owing by the Province to the Service Provider in accordance with Section 15.5 (*Right of Set-Off*) of the Agreement. Any discrepancies that are subsequently discovered regarding the Service Level Credits will be reconciled in the following invoices to be provided by the Service Provider to the Province. If the Parties are unable to agree on all necessary adjustments regarding the Service Level Credits, then either party can raise the issue through the Governance Process for resolution.

10. **Managed Services SLA Termination Events.**

(a) Subject to the provisions of paragraphs (b) to (d) below, and or the purposes of Article 28 *(Default and Termination)* of the Agreement, a "**Service Level Termination Event**" means the failure by the Service Provider to achieve or exceed the Managed Services SLAs set forth below, provided, however, that upon the occurrence of a single Problem that causes a failure in multiple SLAs, only the Single Problem SLA selected by the Province under Section 5 (*Single Problem, Multiple Occurrences*) above shall be used in to determine whether a Service Level Termination Event has occurred:

(i) the occurrence of SLA Failures (that are not subject to an Earnback Credit with respect to the same Managed Services SLA) in each month during any "X" consecutive months, as "X" is designated in the Table below; or

(ii) the occurrence of "Y" SLA Failures (that are not subject to an Earnback Credit with respect to the same managed Services SLAs) within an SLA Group as designated in the Table below within any rolling 12-month period.

Table – SLA Termination Events by SLA Group			
Category	**SLA Group***	**X**	**Y**
Mid Range	MR - A	3	14
Mid Range (If one SLA in SLA Group)	MR - B	3	9
Mid Range (If two SLAs in SLA Group)	MR - B	4	12
Mainframe	MF - A	3	16
Mainframe	MF - B	4	12
Storage and Backup	SB - A	3	8
Storage and Backup	SB - B	4	12

* SLA's are associated with SLA Groups (if applicable) in Appendix 11-A (*Service Level Measurements*).

(b) If the Service Provider is relieved from an SLA Failure by another provision of this Agreement, then such SLA Failure shall not be included for the purposes of determining whether a Service Level Termination Event has occurred.

(c) An SLA Failure for which the Service Provider is not required to pay a Service Level Credit because the Service Provider had earned and applied an Earnback Credit against such SLA Failure, is not and will not be deemed to be, counted for purposes of determining whether a Service Level Termination Event has occurred.

(d) Where a single Problem causes the Service Provider to fail more than one Managed Services SLA, then only one SLA Failure shall be deemed to occur as a result of the single Problem for the purposes of determining whether a Service Level Termination Event has occurred.

(e) For clarification, any and all references in Section 8.9 (*Service Level Failures*) of the Agreement to the failure of the Service Provider to meet an SLA, or such similar references, shall mean the Service Provider's complete failure to provide or otherwise perform the Service to which the SLA applies.

11. **Data Center SLA Termination Events.** Data Center SLA Termination Events are as described in Appendix 11-C (*Data Center Service Levels*).

12. **Remediation Plan.** In addition to the obligations otherwise set forth in Article 8 (*Service Levels*) of the Agreement and in this **Schedule 12** (*Service Level Failures*), in the event of an SLA Failure the Service Provider shall promptly prepare a remediation plan to cure the SLA Failure (the "**Remediation Plan**"), the Service Provider will deliver the Remediation Plan to the Province once available.

SCHEDULE 13

CHANGES TO WEIGHTINGS

(Section 8.9/Schedule 12)

1. **Purpose.** The purpose of this Schedule is to describe the Province's right to change the Weighting attached to the Managed Services SLAs, as contemplated in Section 3(c) of **Schedule 12** (*Service Level Failures*).

2. **Changes to Weightings.** The Province shall have the right, once in each Contract Year quarter, and upon 90 days prior written notice to the Service Provider, to adjust the Weightings allocated to the Managed Services SLAs, subject to the following:

(a) except as set forth in Section 3 (*Change of SLO to SLA*) below, the Province shall not be entitled to make any changes to the Weightings during the period commencing on the Hand-Over Date and expiring eighteen (18) months after the Hand-Over Date;

(b) the aggregate Weightings attached to the Managed Services SLAs shall not exceed two hundred and fifty percent (250%);

(c) the monthly Maximum At Risk Amount shall not be increased;

(d) no Weighting attached to any one Managed Services SLA shall be increased by more than ten percent (10%) at any one time; and

(e) the maximum Weighting attached to any one Managed Services SLA shall not exceed twenty percent (20%).

By way of illustration, below is an example of an absolute change of 10% to a single Managed Services SLA:

Name	Weighting	Change	New Weighting
SLA 1	10%	+10%	20%
SLA 2	20%		20%
SLA 3	20%		20%
SLA 4	20%	-5%	15%
SLA 5	20%	-5%	15%
SLA 6	20%		20%
SLA 7	20%		20%
SLA 8	20%		20%
SLA 9	20%		20%
SLA 10	20%		20%
SLA 11	20%		20%
SLA 12	20%		20%
SLA 13	20%		20%
Total	**250%**		**250%**

3. **Change of SLOs to SLAs.** Notwithstanding the provision if Section 2(a) (*Changes to Weightings*) above, the provisions of this Section 3 below shall apply in respect of the following Managed Services Service Levels: (i) Update to Priority 1 Incident within Target; (ii) Update to Priority 2 Incident

within Target; (iii) Tier 3 Remote Server Availability Service Levels; and (iv) Change Management – Successful Changes:

(a) such Managed Services Service Level shall initially be and be deemed to be an SLO;

(b) commencing with month six (6) following the Hand-Over Date, if there should be three (3) or more Failures in respect of such Managed Services SLO in any rolling six (6) month period, then upon fifteen (15) days written notice to the Service Provider, the Province may:

(i) promote such Managed Services Service Levels from being SLOs to being Service Level Agreements (SLAs) commencing with the next following month; and

(ii) allocate Weightings thereto in accordance with the provisions of Sections 2(b) to 2(e) above (except that the 90 day notice period referred to therein is not applicable); and

(c) if after having been promoted to a Managed Services SLA, the Service Provider achieves such promoted Managed Services SLA in each month for six consecutive months, then:

(i) such promoted Managed Services SLA will revert back to an SLO in the following month without any further act or formality of the Parties; and

(ii) the Province will rebalance the Weightings attached to the managed Services SLAs.

For greater clarification, if the Service Provider does not achieve such promoted Managed Services SLA in a particular month, and as result applies an Earnback Credit against a Service Level Credit in respect of such failed Managed Services SLA, then the Service Provider will still have failed to achieve that promoted Managed Services SLA during that particular month for purposes of this Section 3(c).

SCHEDULE 14
NON-DISCLOSURE AGREEMENT

(See attached)

This Schedule 14 (*Non-Disclosure Agreement*) comprises two forms of non-disclosure agreements for use as follows:

- Schedule 14A - for use in connection with third parties (excluding Province employees) who will have access to Service Provider Confidential Information, as contemplated under the Agreement.

- Schedule 14B – for use in connection with any Benchmarking where the Benchmarker will have access to Service Provider Confidential Information and Province Confidential Information.

SCHEDULE 14A
NON-DISCLOSURE AGREEMENT

THIS AGREEMENT, dated as of _____, is between **EDS ADVANCED SOLUTIONS INC.** ("**EDS**") and _____ (the "**Contractor**").

WHEREAS, pursuant to the terms and conditions of a Master Services Agreement (the "**Master Services Agreement**") dated _____ between EDS and Her Majesty the Queen in right of the Province of British Columbia, as represented by the Minister of Labour and Citizens' Services (the "**Province**"), EDS is providing managed services and data centre services to the Province (collectively the "**Strategic Transformation and Mainframe Services Project**");

AND WHEREAS, as contemplated in the Master Services Agreement, EDS is providing or may provide managed services, co-location services and data centre services to members of the Broader Public Sector (as defined below) (which services, as provided by EDS to the Broader Public Sector, shall be deemed to be part of the Strategic Transformation and Mainframe Services Project for the purposes of this Agreement);

AND WHEREAS the Province has requested EDS to provide the Contractor with access to certain confidential, proprietary, or trade secret information of EDS in connection with the Strategic Transformation and Mainframe Services Project for **[insert purpose of access to confidential information, e.g. performing an audit of [name of Ministry], etc.]** (the "**Business Purpose**");

AND WHEREAS, in consideration of the disclosure of EDS' confidential, proprietary or trade secret information to the Contractor, EDS requires that such information be retained in confidence in accordance with the terms and conditions set forth in this Agreement, and the Contractor agrees to keep such information confidential in accordance with such terms;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficient of which is hereby acknowledged, EDS and the Contractor hereby agree as follows:

1. **Definition**. In this Agreement:

(a) **"EDS Confidential Information"** means any technical, business, financial, personal, employee, operational, scientific, research or other information or data of: (1) EDS; (2) EDS' subcontractors, suppliers or customers; or (3) the affiliates of EDS or its subcontractors, suppliers or customers; in whatsoever form or media, whether in writing, electronic form or communicated orally or visually that, at the time of disclosure or within ten days thereafter is designated as confidential (or like designation) and including:

(i) computer programs in any format whatsoever including the object and source therefor, all related documentation, any modifications to such computer programs and documentation and all draft or development versions of such programs, documentation or modifications;

(ii) personal information of EDS employees, subcontractors, suppliers, agents or representatives;

(iii) information relating to the business or affairs of EDS including:

(1) financial information, purchasing and cost information, price and cost data, price and fee amounts, margins and overheads and quoting, pricing and billing policies, practices, processes and procedures;

(2) EDS forecasts, EDS future plans, EDS potential strategies, EDS budgets and EDS investment opportunities; and

(3) marketing techniques, marketing and development plans, methods of obtaining business and business plans; and

(iv) information relating to EDS' products, services and business processes including information relating to:

(1) research and development projects or plans;

(2) information technology, business process or other infrastructures, environments, networks or security including architectures, configurations, topologies, products, logs, parameters and controls;

(3) EDS' business policies, practices, processes and procedures including all policies, practices, processes and procedures relating to security; and

(4) EDS development tools, know-how, methodologies, templates, processes, technologies or algorithms;

whether communicated before or after the date hereof and whether provided or disclosed, directly or indirectly, by EDS or to which the Contractor obtains access, directly or indirectly, through EDS and including any such information disclosed by the Province or the Broader Public Sector. EDS Confidential Information includes documents, working papers, notes, observations, summaries, explanations or other material prepared by any person and derived from the EDS Confidential Information.

(b) **"Broader Public Sector"** means crown corporations or agencies that are owned directly or indirectly by the Province, and all other levels of government within British Columbia including, without limitation, all municipalities, cities, towns, counties or other political jurisdictions of British Columbia, or any agency, board, council, department, authority, tribunal or commission of the Province or of any of the foregoing, and includes any universities, colleges, schools, school boards, hospitals and health authorities in British Columbia.

2. **Confidentiality**.

(a) **Protection**. The Contractor agrees to hold the EDS Confidential Information in strict confidence, and agrees that it will not disclose, distribute or disseminate the EDS Confidential Information, or documents or information derived therefrom, in any way to any third party. Without limiting the generality of the foregoing, the Contractor agrees that it shall treat such information as confidential and with a degree of care no less than the degree of care that the Contractor employs for the protection of its own confidential information of a similar nature. The Contractor will not use the EDS Confidential Information for its own benefit or the benefit of others, except in connection with the Business Purpose as expressly authorized in this Agreement.

(b) **Restriction**. The Contractor also agrees not to copy EDS Confidential Information which is in documented form except with the written consent of EDS. The Contractor shall not disclose or give access to the EDS Confidential Information to any persons other than the Contractor's employees who have a need to know and are identified on Schedule A. Each such employee of the Contractor shall confirm that he or she has read this Agreement and agrees to be bound by the terms of this Agreement as though such employee were a party hereto and shall indicate such agreement in the manner set forth in Schedule A. Any failure of Contractor's employees to comply with the provisions of this Agreement shall be deemed to be a failure of the Contractor to comply with the provisions of this Agreement and the Contractor shall be liable to EDS in respect thereof.

(c) **Exception**. Section 2(a) (**Protection**) and Section 2(b) (**Restriction**) shall not prevent the Contractor from disclosing information that belongs to the Contractor or that the Contractor can reasonably demonstrate:

(i) was, at the time of disclosure to the Contractor, in the public domain;

(ii) after disclosure to the Contractor, is published or otherwise becomes part of the public domain through no fault of the Contractor;

(iii) was in the possession of the Contractor at the time of disclosure to the Contractor, and was not the subject of a pre-existing confidentiality obligation;

(iv) was disclosed independently to the Contractor by a third party (other than the Province or a member of the Broader Public Sector receiving services from EDS) who, insofar as the Contractor was aware, was not subject to any confidentiality obligations in respect thereof, and in any event, provided that such information was not of a nature that had it been the confidential information of the Contractor, the Contractor would have required that it be kept confidential;

(v) was independently developed by the Contractor without the use of any EDS Confidential Information; or

(vi) is disclosed with the prior written approval of EDS, but only to the extent approved by EDS.

This Agreement shall not prevent the Contractor from disclosing EDS Confidential Information which is required to be disclosed pursuant to the applicable law of Canada (including pursuant to a requirement of a governmental agency or law of Canada, or any governmental or political subdivision thereof), so long as the Contractor provides EDS with prompt written notice of such requirement and takes steps sufficient to allow EDS an opportunity to object to such disclosure. Any such disclosure pursuant to applicable law of Canada will only be to the extent legally required and only for the purpose of compliance with applicable law and not for any other purpose.

(d) **Disclosure to the Province**. Section 2(a) (**Protection**) and Section 2(b) (**Restriction**) shall not prevent the Contractor from disclosing EDS Confidential Information to the Province in connection with the Business Purpose.

(e) **Notification of Unauthorized Use of EDS Confidential Information**. The Contractor shall (i) promptly notify EDS of any unauthorized possession, use or disclosure, or attempt to

effect the same, of EDS Confidential Information ("**Unauthorized Disclosure**"), (ii) promptly furnish EDS with details of such Unauthorized Disclosure, and assist EDS in investigating or preventing any recurrence, (iii) cooperate with EDS in any litigation and investigation against third parties deemed necessary by EDS to protect the EDS Confidential Information, as such litigation or investigation is related to the Unauthorized Disclosure, and (iv) promptly use reasonable efforts to prevent a recurrence of any Unauthorized Disclosure.

(f) **Canadian Institute of Chartered Accountants**. If the Contractor is a member in good standing of the Canadian Institute of Chartered Accountants and is acting in such capacity with respect to the EDS Confidential Information disclosed to the Contractor in connection with the Business Purpose, then the Contractor may also disclose EDS Confidential Information to the extent such disclosure is required under any professional standards promulgated by the Canadian Institute of Chartered Accountants. Any such disclosure pursuant to any professional standards promulgated by the Canadian Institute of Chartered Accountants will only be to the extent required under such standards and only for the purpose of compliance therewith and not for any other purpose. In such event, the Contractor shall also be entitled to retain such copies of EDS Confidential Information as is necessary to comply with the professional standards described above with respect to the documentation of work performed, which EDS Confidential Information shall continue to be subject to the provisions of this Agreement.

3. **Return of EDS Confidential Information**. The Contractor shall be entitled to retain one copy of the EDS Confidential Information and any working papers of the Contractor related thereto in its files, which EDS Confidential Information shall continue to be subject to the provisions of this Agreement. Subject to the foregoing, upon the completion of the Business Purpose or at the request of EDS, the Contractor shall return all copies of the EDS Confidential Information, and all derivatives thereof, to EDS or, at EDS' option and direction, shall certify in writing that all copies of the EDS Confidential Information have been destroyed. The Contractor may return the EDS Confidential Information, or any part thereof, to EDS at any time.

4. **No Warranty**. EDS makes no representation or warranty, express or implied, with respect to the EDS Confidential Information and accepts no responsibility for any expenses, losses, or actions incurred or undertaken by the Contractor as a result of the receipt or use of the EDS Confidential Information.

5. **No Further Rights**. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in the EDS Confidential Information except as expressly provided herein.

6. **Injunctive Relief**. The Contractor acknowledges and agrees that the EDS Confidential Information is the confidential, proprietary and trade secret information of EDS or its subcontractors, suppliers or customers or of its or their affiliates and that the unauthorized use or disclosure of the EDS Confidential Information could cause irreparable harm and significant injury to EDS for which EDS would have no adequate remedy at law. Therefore, EDS shall have the right, in addition to any other rights EDS may have at law or in equity, to seek immediate injunctive relief enjoining any breach or potential breach of this Agreement by the Contractor. The Contractor hereby waives the necessity of the posting any form of bond relating to the issuance of injunctive relief.

7. **Media Releases**. No media releases, public announcements or disclosures relating to this Agreement, its subject matter or the EDS Confidential Information shall be issued by the Contractor without the prior written approval of EDS.

8. **Miscellaneous**.

(a) Each of the parties hereto will promptly do, make, execute or deliver, or cause to be done, made, executed or delivered, all such further acts, documents and things as the other party hereto may reasonably require from time to time for the purpose of giving effect to this Agreement and will use reasonable efforts and take all such steps as may be reasonably within its power to implement to their full extent the provisions of this Agreement.

(b) No delay or omission by EDS to exercise any right or power hereunder shall impair such right or power or be construed to be a waiver thereof. All remedies provided for in this Agreement shall be cumulative and in addition to and not in lieu of any other remedies available at law, in equity or otherwise.

(c) Any notices required by this Agreement shall be given in hand or sent by courier, to the applicable address set forth below the names of the parties on the signature page of this Agreement. Either party may from time to time specify as its address for purposes of this Agreement any other address upon giving written notice thereof to the other party.

(d) Subject to the express limitations set out in this Agreement, this Agreement shall enure to the benefit of and be binding upon the parties and their respective successors and permitted assigns.

(e) The word "includes" and words derived from the word "include" are used for illustrative purposes only and are not meant to be limiting.

(f) This Agreement (i) is the complete and exclusive statement between the parties with respect to the protection of the confidentiality of the EDS Confidential Information, (ii) supersedes all related discussions and other communications between the parties, (iii) may only be modified in writing by authorized representatives of the parties, and (iv) shall be governed by the laws of the Province of British Columbia.

(g) This Agreement may be signed in counterparts and each of such counterparts will constitute an original document and such counterparts, taken together, will constitute one and the same instrument.

IN WITNESS WHEREOF, EDS and the Contractor have each caused this Agreement to be signed and delivered as of the date first set forth above.

EDS ADVANCED SOLUTIONS INC.

_____
[Print Name of Contractor]

By:_____ By:_____

Name:

Title: Title:

EDS Advanced Solutions Inc. Vancouver Island Technology Park 2200-4464 Markham Road Victoria, British Columbia V8Z 7X8 Attention: Vice-President, Finance and Administration Telephone: 250-405-2500 Telecopier: 250-405-2563	Name: Address: Attention: Telephone: Telecopier:

SCHEDULE A

Contractor employees granted access to EDS Confidential Information

Designated Persons:

NAME	INITIALS
	(For the purpose of acknowledging that the Designated Person has read and understands the restrictions contained in the Agreement and agrees to be bound by such restrictions)
1. John Smith – ABC Inc.	_____

SCHEDULE 14B
NON-DISCLOSURE AGREEMENT

THIS AGREEMENT, dated as of _____, is among **EDS ADVANCED SOLUTIONS INC.** ("**EDS**"), **Her Majesty the Queen in Right of the Province of British Columbia as represented by the Minister of Labour and Citizens' Services** (the "**Province**") and _____ (the "**Contractor**").

WHEREAS, pursuant to the terms and conditions of a Master Services Agreement (the "**Master Services Agreement**") dated _____ between EDS and Her Majesty the Queen in right of the Province of British Columbia, as represented by the Minister of Labour and Citizens' Services (the "**Province**"), EDS is providing managed services and data centre services to the Province (collectively the "**Strategic Transformation and Mainframe Services Project**");

AND WHEREAS, as contemplated in the Master Services Agreement, EDS is providing or may provide managed services, co-location services and data centre services to members of the Broader Public Sector (as defined below) under a separate agreement directly with such Broader Public Sector entity (the "**BPS Services Agreement**"), which services, as provided by EDS to the Broader Public Sector, shall be deemed to be part of the Strategic Transformation and Mainframe Services Project for the purposes of this Agreement;

AND WHEREAS the Province has requested EDS to provide the Contractor with access to certain confidential, proprietary, or trade secret information of EDS in connection with the Strategic Transformation and Mainframe Services Project for the purpose of performing a benchmarking of the services and fees under the Master Services Agreement and **[insert appropriate details regarding the benchmarking]** (the "**Business Purpose**");

AND WHEREAS, in consideration of the disclosure of EDS' and the Province's confidential, proprietary or trade secret information to the Contractor, EDS and the Province requires that such information be retained in confidence in accordance with the terms and conditions set forth in this Agreement, and the Contractor agrees to keep such information confidential in accordance with such terms;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficient of which is hereby acknowledged, EDS, the Province and the Contractor hereby agree as follows:

1. **Definition**. In this Agreement:

(a) **"EDS Confidential Information"** means any technical, business, financial, personal, employee, operational, scientific, research or other information or data of: (1) EDS; (2) EDS' subcontractors, suppliers or customers; or (3) the affiliates of EDS or its subcontractors, suppliers or customers; in whatsoever form or media, whether in writing, electronic form or communicated orally or visually that, at the time of disclosure or within ten days thereafter is designated as confidential (or like designation) and including:

(i) computer programs in any format whatsoever including the object and source therefor, all related documentation, any modifications to such computer programs and documentation and all draft or development versions of such programs, documentation or modifications;

(ii) personal information of EDS employees, subcontractors, suppliers, agents or representatives;

(iii) information relating to the business or affairs of EDS including:

(1) financial information, purchasing and cost information, price and cost data, price and fee amounts, margins and overheads and quoting, pricing and billing policies, practices, processes and procedures;

(2) EDS forecasts, EDS future plans, EDS potential strategies, EDS budgets and EDS investment opportunities; and

(3) marketing techniques, marketing and development plans, methods of obtaining business and business plans; and

(iv) information relating to EDS' products, services and business processes including information relating to:

(1) research and development projects or plans;

(2) information technology, business process or other infrastructures, environments, networks or security including architectures, configurations, topologies, products, logs, parameters and controls;

(3) EDS' business policies, practices, processes and procedures including all policies, practices, processes and procedures relating to security; and

(4) EDS development tools, know-how, methodologies, templates, processes, technologies or algorithms;

whether communicated before or after the date hereof and whether provided or disclosed, directly or indirectly, by EDS or to which the Contractor obtains access, directly or indirectly, through EDS and including any such information disclosed by the Province or the Broader Public Sector. EDS Confidential Information includes documents, working papers, notes, observations, summaries, explanations or other material prepared by any person and derived from the EDS Confidential Information.

(b) **"Broader Public Sector"** means crown corporations or agencies that are owned directly or indirectly by the Province, and all other levels of government within British Columbia including, without limitation, all municipalities, cities, towns, counties or other political jurisdictions of British Columbia, or any agency, board, council, department, authority, tribunal or commission of the Province or of any of the foregoing, and includes any universities, colleges, schools, school boards, hospitals and health authorities in British Columbia.

(c) **"Confidential Information"** means the EDS Confidential Information and the Province Confidential Information.

(d) **"Province Confidential Information"** means any technical, business, financial, personal, employee, operational, scientific, research or other information or data of the Province, and any other information regarding the Province's business, plans and markets, information of or

relating to the Province, the Broader Public Sector or of any person that has disclosed such information to the Province or its agents, in whatsoever form or media, whether in writing, in electronic form or communicated orally or visually that, at the time of disclosure is designated or within ten days thereafter is designated as confidential (or like designation), whether communicated before or after the date hereof and whether provided or disclosed, directly or indirectly, by the Province or the Broader Public Sector or to which the Contractor obtains access, directly or indirectly, through the Province or the Broader Public Sector and including any such information disclosed by the Province or the Broader Public Sector. Province Confidential Information includes documents, working papers, notes, observations, summaries, explanations or other material prepared by any person and derived from the Province Confidential Information.

2. **Confidentiality.**

(a) **Protection**. The Contractor agrees to hold the Confidential Information in strict confidence, and agrees that it will not disclose, distribute or disseminate the Confidential Information, or documents or information derived therefrom, in any way to any third party. Without limiting the generality of the foregoing, the Contractor agrees that it shall treat such information as confidential and with a degree of care no less than the degree of care that the Contractor employs for the protection of its own confidential information of a similar nature. The Contractor will not use the Confidential Information for its own benefit or the benefit of others, except in connection with the Business Purpose as expressly authorized in this Agreement.

(b) **Restriction**. The Contractor also agrees not to copy Confidential Information which is in documented form except with the written consent of the Province and EDS. The Contractor shall not disclose or give access to the Confidential Information to any persons other than the Contractor's employees who have a need to know and are identified on Schedule A. Each such employee of the Contractor shall confirm that he or she has read this Agreement and agrees to be bound by the terms of this Agreement as though such employee were a party hereto and shall indicate such agreement in the manner set forth in Schedule A. Any failure of Contractor's employees to comply with the provisions of this Agreement shall be deemed to be a failure of the Contractor to comply with the provisions of this Agreement and the Contractor shall be liable to the Province and EDS in respect thereof.

(c) **Exception**. Section 2(a) (**Protection**) and Section 2(b) (**Restriction**) shall not prevent the Contractor from disclosing information that belongs to the Contractor or that the Contractor can reasonably demonstrate:

(vii) was, at the time of disclosure to the Contractor, in the public domain;

(viii) after disclosure to the Contractor, is published or otherwise becomes part of the public domain through no fault of the Contractor;

(ix) was in the possession of the Contractor at the time of disclosure to the Contractor, and was not the subject of a pre-existing confidentiality obligation;

(x) was disclosed independently to the Contractor by a third party (other than the Province or a member of the Broader Public Sector receiving services from EDS) who, insofar as the Contractor was aware, was not subject to any confidentiality obligations in respect thereof, and in any event, provided that

such information was not of a nature that had it been the confidential information of the Contractor, the Contractor would have required that it be kept confidential;

(xi) was independently developed by the Contractor without the use of any Confidential Information; or

(xii) is disclosed with the prior written approval of the Province, for the Province Confidential Information, and EDS, for the EDS Confidential Information, but only to the extent approved by those parties.

This Agreement shall not prevent the Contractor from disclosing Confidential Information which is required to be disclosed pursuant to the applicable law of Canada (including pursuant to a requirement of a governmental agency or law of Canada, or any governmental or political subdivision thereof), so long as the Contractor provides the Province and EDS with prompt written notice of such requirement and takes steps sufficient to allow the Province and EDS an opportunity to object to such disclosure. Any such disclosure pursuant to applicable law of Canada will only be to the extent legally required and only for the purpose of compliance with applicable law and not for any other purpose.

(d) **Disclosure to the Province**. Section 2(a) (**Protection**) and Section 2(b) (**Restriction**) shall not prevent the Contractor from disclosing Confidential Information to the Province and EDS in connection with the Business Purpose.

(e) **Notification of Unauthorized Use of EDS Confidential Information**. The Contractor shall (i) promptly notify the Province and EDS of any unauthorized possession, use or disclosure, or attempt to effect the same, of Confidential Information ("**Unauthorized Disclosure**"), (ii) promptly furnish the Province and EDS with details of such Unauthorized Disclosure, and assist the Province and EDS in investigating or preventing any recurrence, (iii) cooperate with EDS in any litigation and investigation against third parties deemed necessary by EDS to protect the EDS Confidential Information, as such litigation or investigation is related to the Unauthorized Disclosure, and (iv) promptly use reasonable efforts to prevent a recurrence of any Unauthorized Disclosure.

3. **Return of EDS Confidential Information**. The Contractor shall be entitled to retain one copy of the Confidential Information and any working papers of the Contractor related thereto in its files, which Confidential Information shall continue to be subject to the provisions of this Agreement. Subject to the foregoing, upon the completion of the Business Purpose or at the request of the Province or EDS, the Contractor shall return all copies of the Province Confidential Information and the EDS Confidential Information to the Province and EDS, respectively, and all derivatives thereof, or, at the Province's or EDS' option with respect to their own confidential information, the Contractor will certify in writing that all copies of the Confidential Information have been destroyed. The Contractor may return the Province Confidential Information and the EDS Confidential Information, or any part thereof, to the Province or EDS, respectively, at any time.

4. **No Warranty**. Neither the Province nor EDS makes any representation or warranty, express or implied, with respect to their Confidential Information and neither the Province nor EDS accepts responsibility for any expenses, losses, or actions incurred or undertaken by the Contractor as a result of the receipt or use of the Confidential Information.

5. **No Further Rights**. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in the Confidential Information except as expressly provided herein.

6. **Injunctive Relief**. The Contractor acknowledges and agrees that the Confidential Information is the confidential, proprietary and trade secret information of EDS (or its subcontractors, suppliers or customers or of its or their affiliates) and the Province and that the unauthorized use or disclosure of the EDS Confidential Information or the Province Confidential Information could cause irreparable harm and significant injury to EDS and the Province, respectively, for which neither EDS nor the Province would have no adequate remedy at law. Therefore, each of the Province and EDS shall have the right, in addition to any other rights they may have at law or in equity, to seek immediate injunctive relief enjoining any breach or potential breach of this Agreement by the Contractor. The Contractor hereby waives the necessity of the posting any form of bond relating to the issuance of injunctive relief.

7. **Media Releases**. No media releases, public announcements or disclosures relating to this Agreement, its subject matter or the Confidential Information shall be issued by the Contractor without the prior written approval of the Province and EDS.

8. **Miscellaneous**.

   (a) Each of the parties hereto will promptly do, make, execute or deliver, or cause to be done, made, executed or delivered, all such further acts, documents and things as the other party hereto may reasonably require from time to time for the purpose of giving effect to this Agreement and will use reasonable efforts and take all such steps as may be reasonably within its power to implement to their full extent the provisions of this Agreement.

   (b) No delay or omission by the Province or EDS to exercise any right or power hereunder shall impair such right or power or be construed to be a waiver thereof. All remedies provided for in this Agreement shall be cumulative and in addition to and not in lieu of any other remedies available at law, in equity or otherwise.

   (c) Any notices required by this Agreement shall be given in hand or sent by courier, to the applicable address set forth below the names of the parties on the signature page of this Agreement. Either party may from time to time specify as its address for purposes of this Agreement any other address upon giving written notice thereof to the other party.

   (d) Subject to the express limitations set out in this Agreement, this Agreement shall enure to the benefit of and be binding upon the parties and their respective successors and permitted assigns.

   (e) The word "includes" and words derived from the word "include" are used for illustrative purposes only and are not meant to be limiting.

   (f) This Agreement (i) is the complete and exclusive statement between the parties with respect to the protection of the confidentiality of the Confidential Information, (ii) supersedes all related discussions and other communications between the parties, (iii)

may only be modified in writing by authorized representatives of the parties, and (iv) shall be governed by the laws of the Province of British Columbia.

(g) This Agreement may be signed in counterparts and each of such counterparts will constitute an original document and such counterparts, taken together, will constitute one and the same instrument.

IN WITNESS WHEREOF, EDS, the Province and the Contractor have each caused this Agreement to be signed and delivered as of the date first set forth above.

EDS ADVANCED SOLUTIONS INC.

By:_____

Name:

Title:

_____
[Print Name of Contractor]

By:_____

Name:

Title:

EDS Advanced Solutions Inc. Vancouver Island Technology Park 2200-4464 Markham Road Victoria, British Columbia V8Z 7X8 Attention: Vice-President, Finance and Administration Telephone: 250-405-2500 Telecopier: 250-405-2563	Name: Address: Attention: Telephone: Telecopier:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Minister of Labour and Citizens' Services:

By:_____
Name:
Title:

Her Majesty the Queen in Right of the Province of British Columbia Ministry of Labour and Citizens' Services Workplace Technology Services 4000 Seymour Place Victoria, British Columbia V8X 1W5 AND: PO Box 9412 Stn. Prov Govt Victoria, British Columbia V8W 9V1 Attention: Executive Director, Alliance Management Office Telephone: 250- Telecopier: 250-	

SCHEDULE A

Contractor employees granted access to EDS Confidential Information and Province Confidential Information

Designated Persons:

NAME	INITIALS
	(For the purpose of acknowledging that the Designated Person has read and understands the restrictions contained in the Agreement and agrees to be bound by such restrictions)
1. John Smith – ABC Inc.	_____

SCHEDULE 15

CONDITIONS OF USE OF PROVINCE MARKS

(Section 10.2)

The display or use by the Service Provider of the Province Marks shall conform to the following, to the extent applicable to such display or use:

(a) the applicable provisions of this Agreement and the Transaction Documents,

(b) the *Province Symbols and Honours Act (http://www.qp.gov.bc.ca/statreg/stat/P/96380_01.htm)* , to the extent applicable;

(c) the Visual Identity and Graphic Standards for B.C. Government Websites, provided that the impact on the Service Provider's display or use of the Province Marks as a result of any changes to the Visual Identity and Graphic Standards for B.C. Government Websites shall be implemented in accordance with the Change Order Process; and

(d) any relevant Province policies as directed by the Province in accordance Section 11.4 (*Province's Right to Issue Directives*) of the Agreement.

SCHEDULE 16

PROVINCE MARKS

(Section 10.1)

The Province hereby consents to the Service Provider providing, and the Service Provider shall provide, the Data Centre Services and the Managed Services under the Province Mark set forth below (or such other Province Mark as may be requested by the Province from time to time through the Change Order Process), in accordance with Section 12.1 (*Province Marks*) and **Schedule 15** *(Conditions of Use of Province Marks)*. For greater clarification, and notwithstanding the foregoing, the Service Provider shall also identify itself in all communications and correspondence with Clients and Stakeholders in the manner required pursuant to the provisions of the *Business Practices and Consumer Protection Act* (British Columbia). Other than Broader Public Sector entities, the Province agrees that it will not authorize or license any other third Person to use the Province Mark during the Term (provided that the Province has not required the Service Provider to use another Province Mark in substitution for such mark) in connection with the Services. Such agreement shall not restrict the Province's rights to use the Province Mark or to license or use any other Province Mark including marks similar thereto.

Province Mark

"Hosting Solutions BC"
"Hosting Solutions B.C."
"Hosting Solutions of British Columbia"
"Hosting Solutions British Columbia"

SCHEDULE 17

COMMUNICATIONS PLAN AND PROCESS

(Section 10.5)

1. Definitions. Capitalized terms used in this **Schedule 17** (*Communication Plan and Process*) that are not defined within this Schedule will have the meanings given to such terms set forth in **Schedule 1** (*Definitions*) to the Agreement.

2. Purpose of Schedule. This Schedule defines and describes the approach the Parties will use to facilitate the effective communications necessary to the success of this Agreement.

3. Communication Principles.

3.1 ***General*** - The Parties agree that effective communications are a key component to the success of the arrangement with respect to the Agreement. The communications approach will:

(a) provide clear direction to the Parties as to the responsibilities and key processes for comprehensive communications;

(b) outline the communication process and activities that will occur during the Term;

(c) identify the respective Parties responsible for each type of communication;

(d) recognize the importance of mutual understanding and respect for the lines of authority of each Party;

(e) adhere to the governance structure described in Article 11 (*Relationship Management and Human Resources*) and **Schedule 18** (*Governance*) of the Agreement; and

(f) be consistent with the terms of this Agreement.

3.2 ***Communications between Parties*** - Communication between the Parties will take place at various levels within the respective organizations through formal, informal, and ad hoc arrangements and will:

(a) ensure knowledge of relevant activities, issues, and problems is shared by both Parties;

(b) ensure proper discussion, resolution and escalation of issues;

(c) ensure reasonable responses are provided within reasonable timeframes; and

(d) facilitate issue resolution at the lowest appropriate level of the governance model.

3.3 ***Written Communications*** - The Parties agree that, at a minimum, those communications that have the potential to result in changes related to policy, scope, contract terms, or approvals should be in writing and otherwise be in accordance with the terms of the Agreement.

3.4 ***Direction of the Province*** - The Service Provider will follow the Province's prescribed policies and direction regarding development, content and distribution of verbal and written communications in connection with this Agreement with the Clients and Stakeholders, and the public and the media.

3.5 ***Resources*** - Both Parties will:

(a) provide the appropriate staff resources necessary to communicate on a regular basis through routine meetings and written documentation of meeting outcomes as required; and

(b) work collaboratively to ensure that any review and approval processes do not unduly delay development, completion or distribution of communications.

The Communication Plan may be modified and supplemented during the course of the Term pursuant to the Change Order Process to better facilitate the effective communications necessary to the success of this Agreement.

4. Communications between the Province and the Service Provider. The Parties will engage in ongoing communication with each other to establish communication roles, including defining authority, functions and process, all governed in accordance with the terms set forth in **Schedule 17** (*Communication Plan and Process*) of this Agreement.

5. Service Provider Communication with Stakeholders.

5.1 ***Communications Plan*** - The Parties will:

(a) prepare and implement a detailed form of the Communications Plan, with preparation and implementation of the Communication Plan to start March 30, 2009;

(b) amend and supplement the detailed Communications Plan within three months after the Handover Date; and

(c) amend and supplement the Communications Plan annually thereafter, or more frequently as may be appropriate.

5.2 ***Stakeholders*** - Notwithstanding anything herein to the contrary and despite any delegation of responsibilities, the Province will retain control over communications with Clients and Stakeholders. Communications with Stakeholders, which are Broader Public Sector entities that have not entered into a BPS Services Agreement with the Service Provider, will be conducted in accordance with the provisions of Schedule 26 (*Growth and Marketing*).

6. Public Communications. The Parties will jointly develop a communication strategy to deal with the public. The Parties acknowledge and agree that press releases issued individually or jointly shall be issued in accordance with Section 10.4 (*Publicity*) of the Agreement. The Service Provider will refer any inquiries from the public or governmental bodies related to this Agreement to the Province's Business Relationship Executive, Strategic Infrastructure, or as otherwise directed by the Province.

7. Media Contact. The Service Provider will not initiate or respond to calls from the media concerning any aspect of the Agreement or the Services, unless specifically authorized by the Province in writing to do so. The Service Provider will immediately refer any calls from the media to the Province's Business Relationship Executive, Strategic Infrastructure, or as otherwise directed by the Province.

8. Branding. See Article 10 (*Branding and Communications*) of the Agreement.

SCHEDULE 18

GOVERNANCE

(Section 11.1)

1. **General**

1.1 **Purpose.** This Schedule 18 (*Governance*) sets forth the overarching governance framework for the effective implementation of the Agreement, which will be facilitated by the Province and the Service Provider through joint direction and control and joint management through a defined areas of responsibility and authority. The intent of the governance framework is to facilitate:

(a) the achievement and monitoring of the objectives of the Parties as set forth in Section 1.13 (*Objectives of the Parties*) of the Agreement;

(b) the effective implementation of the Agreement, including the growth of participation by the Broader Public Sector; and

(c) the development of productive organizational relationships, including relationship management, through processes that support "best practice" joint governance.

1.2 **Objectives of the Governance Framework.** The primary objectives of the governance framework are to continually ensure that:

(a) the value proposition derived from the Agreement is consistent with the expectations of the Province and the Service Provider;

(b) the strategies and plans of the Province and the Service Provider, to the extent that such strategies and plans will have an impact on the Agreement, are understood by all;

(c) effective contract and service management processes exist, including, change, problem, and crisis management, request for service and contract amendment; and

(d) an effective relationship management process exists including communication, decision making, reporting, measurement, issue resolution and dispute resolutions processes.

1.3 **Guiding Principles.** The Parties agree to adhere to the following guiding principles:

(a) proactively identify sources of disagreement and discord and take timely action before they become matters of dispute;

(b) endeavor to be sensitive to activities that may be of concern to the others, providing early notice that it wishes to pursue such activity and will engage in consultation about such activity;

(c) where possible, resolve issues through a process of cooperative and amicable negotiations;

(d) ensure that the governance framework enables the Province and Service Provider to:

(i) understand and execute their responsibilities and accountabilities under the Agreement;

(ii) subject to the specific rights of a Party set out in the Agreement, work co-operatively together over the entire Term of the Agreement;

(iii) subject to the specific rights of a Party set out in the Agreement, make decisions guided by what is best for the on-going management and delivery of high quality Services;

(iv) subject to the specific restrictions set out in the Agreement, have access to the information necessary to fulfill their obligations under the Agreement;

(v) subject to the specific rights of a Party set out in the Agreement, develop and maintain high quality relationships;

(vi) effectively identify and resolve difficult issues;

(vii) accommodate the lifecycle of the Agreement;

(viii) allow the Province and Service Provider to acknowledge and act in ways that are consistent with their complex and varied roles and responsibilities pursuant to the Agreements;

(ix) clarify and facilitate ongoing relationships with Province, Clients, Buyers and Stakeholders;

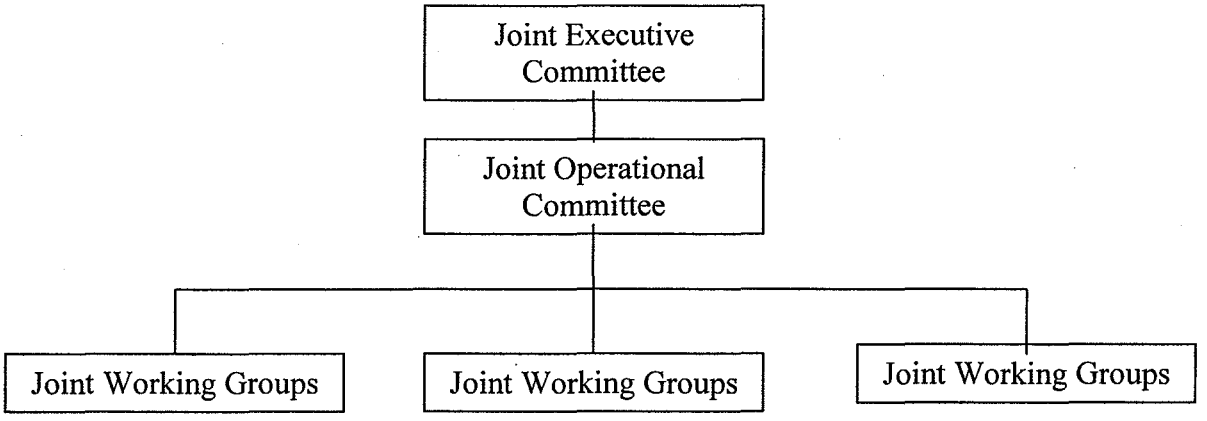
(x) ensure that the Province's and Service Provider's detailed knowledge about the Services is retained; and

(xi) end a relationship responsibly when appropriate.

1.4 **Participation in Governance Process.** The Province and the Service Provider agree that they will each utilize the Governance Process in accordance with the provisions of this Schedule including by requiring its representatives to attend meetings and to participate in the activities of the committees of which they are members in accordance with this Schedule.

2. Governance Framework

The overall governance framework is depicted as follows:



2.1 **Authority and Decision Making.** The following table outlines, at a high level, the scope of authority and decision making of the various committees, teams and project working groups described in the governance framework. Any decision made by a governance committee, that is within the operating mandate of that committee will be:

(a) made by the mutual consensus of the Province committee members on the one hand, and the Service Provider committee members on the other hand; and

(b) binding upon the Parties (unless decided otherwise by a committee having authority to do so).

Decisions that extend beyond the mandate of the committee will be escalated to the next appropriate committee as indicated in this Schedule, and where no such committee is indicated, to the Joint Executive Committee. All decisions made by the committees will, where appropriate, follow the Change Order Process. All decisions will be recorded in meeting minutes and a notice of decision will be sent to all committee members.

GOVERNANCE COMMITTEE	AUTHORITY TO MAKE DECISIONS
Joint Executive Committee	Issues that significantly impact: - the relationship of the Parties - scope of the Services - transition and transformation under the Transition Plan and the Transformation SOW - financial matters Issues impacting the Parties including: - Legislative - Policy - Privacy and security Issues escalated from the Joint Operations Committee.
Joint Operations Committee	Issues that impact: - scope, including changes to SOW Documents and new projects - timeframes - budget management - Client relations - performance and Service Levels - resource sufficiency and availability - human resources/change management issues Issues escalated from Joint Working Groups
Joint Working Groups	Day to day decisions and issue resolution for items within the scope of their respective mandates as defined in their charters (no decision making authority unless delegated).

2.2 **Continuing Obligations of the Parties.** Notwithstanding any other provision of this Schedule, the purpose of the governance framework set forth in this Schedule is to facilitate communications between the Parties regarding the ongoing Services under the Agreement and dispute resolution. Nothing in this Schedule nor any action or omission of the Parties pursuant to this Schedule shall alter or amend the Parties' respective responsibilities regarding the Services as set forth in the Agreement or the applicable Schedules.

3. Joint Governance Structure

The Province and the Service Provider have the responsibility to govern all aspects of the Agreement including the provision of the Services to the Province as contemplated under the Agreement. This responsibility will be executed through three levels of joint committees: Joint Executive Committee, Joint Operations Committee, and Joint Working Groups.

3.1 **Joint Executive Committee (JEC).** The executive committee ("Joint Executive Committee" or "JEC") will function as the executive level governance body for the Agreement and for the provision of the Services to the Province under the Agreement. The JEC will have responsibility for oversight of the Agreement and the relationship between the Province and the Service Provider and will ensure that the Agreement continues to be aligned with and enable such strategies and plans.

(a) ***Composition of the JEC.***

(i) Province (4 members): Deputy Minister, MLCS (Chair); ADM, Strategic Infrastructure; ADM, Alternative Service Delivery Secretariat; ADM, WTS

(ii) Service Provider (4 members): Vice-President and General Manager, EDS Canada; Vice-President, Public Sector, EDS Canada; Vice-President, Public Sector, B.C., EDS Canada; President, EDS Advanced Solutions

Other employees, consultants, or advisors of the Province and the Service Provider may attend meetings of the JEC at the invitation of either Party to the extent reasonably necessary to sufficiently address matters for discussion on the agenda of a JEC meeting. The JEC may also invite Buyers and industry and government leaders to participate in such meetings to facilitate information exchange and increase the value of the strategies discussed.

(b) ***Chair of the JEC.*** The Chair of the JEC meetings shall be a representative of the Province, who is a member of the JEC.

(c) ***Changes in Composition of the JEC.*** Each of the Parties may from time to time change its respective representatives on the JEC by providing written notice to the other Party of such change. Notwithstanding such right to replace individuals, the parties agree that such replacements shall be of a similar or greater authority unless otherwise agreed by the other Party.

(d) ***Meetings of the JEC.*** The JEC shall hold meetings or telephone or video conferences at least four times per year, with at least two of such meetings in each contract year being face-to-face meetings. The JEC may meet more frequently, as the members of such committee may determine in their reasonable discretion.

(e) ***Special Meetings of the JEC.*** Notwithstanding the foregoing, the chair of the JEC may call a special meeting to consider any relevant issue upon reasonable prior notice to the other members of the JEC, such notice shall set forth the matters to be discussed or determined at such special meeting. A special meeting of the JEC, once called, shall be convened as soon as reasonably practical.

(f) ***Quorum.*** A quorum for any meeting of the JEC shall be four members comprising at least two representatives of each Party.

(g) ***Roles of the JEC.*** The responsibilities of the JEC are to:

(i) provide oversight for the Agreement and the relationship between the Province and the Service Provider as parties to the Agreement;

(ii) provide leadership on behalf of all of the Buyers by:

(A) consistently encouraging the shared services strategy and the outsourcing relationship,

(B) clarifying accountabilities, and

(C) addressing barriers and issues that are beyond the ability of management to resolve.

(h) ***Responsibilities of the JEC.*** The activities of the JEC will include, without limitation:

(i) sharing and understanding the strategies and plans of the Province, Buyers and the Service Provider as they relate to the Agreement,

(ii) identifying potential upcoming changes that will need to be managed, reviewing and refreshing the strategic goals for the alternative service delivery relationship consistent with those changes, and discussing strategies to leverage the relationship of the Buyers and the Service Provider to provide increased value and to solve business problems,

(iii) reviewing performance (for example, Services, Service Levels, transformation, growth, and relationship) against plans,

(iv) approving the following on an annual basis with respect to WTS: joint annual objectives, Committed Annual Plan, JMC Business Development Plan,

(v) ensuring that there is sufficient transparency of the financials,

(vi) ratifying and where appropriate recommending changes to the Agreement and how it is being managed,

(vii) addressing matters that were escalated to it within the time period set forth in Section 27.1 (*Informal Dispute Resolution*) of the Agreement;

(viii) addressing matters expressly referred to the JEC under the Agreement, including:

- Mandatory Change Requests;
- Approval of a Material Subcontractor;
- changes in Service Provider Key Positions;
- removal of a Material Subcontractor or Access Subcontractor under Section 12.13 (*Removal of Subcontractor*); and
- such other matters as may be referred to the JEC in the Agreement;

(ix) pursuant to Section 12.11 (*Consent to Use of Material Subcontractors*) of the Agreement, where the Province does not Approve a Material Subcontractor submitted by Service Provider, provide the rationale for such non-Approval to the Service Provider during the next JEC meeting and such rationale shall be included in the minutes of the appropriate JEC meeting.

(i) ***Decisions and Approvals of the JEC.*** The decisions and approvals of the JEC will be made in accordance with the decision and approval rights set out in the Agreement. Decisions or approvals specifically assigned in the Agreement to the JEC, or other decisions which may come to the JEC, will, to the extent possible, be made by consensus. When consensus cannot be achieved, the parties will have the option to strike a Special Joint Committee (see below) or to pursue other dispute resolution mechanisms set out in Article 27 (*Dispute Resolution*) of the Agreement; and

(j) ***Rules of Procedure and Protocols.*** In addition to the provisions of this Schedule 18 (Governance) and subject to the provisions of the Agreement, the JEC may develop its own rules of procedures and protocol.

3.2 **Committees of the JEC.** The JEC shall have the discretion to form a joint committee for any purpose it deems appropriate, taking into consideration its mandate and any applicable terms, conditions or restrictions set out in the Agreement. As of the Hand-Over Date, the following joint committees are contemplated under the JEC, and with respect to paragraph (b), such committees shall be established as of the Hand-Over Date:

(a) ***Special Joint Committee.*** The JEC may, on an ad hoc basis, form a special joint committee (the "**Special Joint Committee**") to ensure objective review of areas of specific concern, including when a difference or dispute cannot be resolved within the governance structure. Depending on the subject under consideration, the Special Joint Committee will be composed of members of senior management of the parties, JEC members, Buyers, and/or specialists on the topic (for example, financial officers or information technologists), and if the Parties wish, a mediator or facilitator with a knowledge of the subject.

The costs for the mediator or facilitator will be shared equally between the parties. The JEC will appoint a chair of the Special Joint Committee, define the scope of its deliberations, and request a time for the Special Joint Committee to report back to the JEC with its recommendations.

(b) **Joint Marketing Committee (JMC).** The JEC will establish a joint marketing committee (the "**Joint Marketing Committee**" or "**JMC**") which will report to the Joint Executive Committee for the general purpose of ensuring that there are adequate and appropriate resources and processes in place to ensure the growth of the data centre and managed services provided under the Agreement.

(i) ***Composition of the JMC.***

(A) Province: ADM, SI; Business Relationship Executive, SI (Chair); Executive Director, Client Service, WTS; Executive Director, AMO, WTS

(B) the Service Provider: EDS Advanced Solutions STMS Project Lead; Client Sales Executive; Head, EAS Advanced Solutions CRM Team

(ii) ***Chair of the JMC.*** The Chair of the JMC shall be a representative of the Province, who is a member of the JEC.

(iii) ***Meetings of the JMC.*** The JMC shall hold meetings or telephone or video conferences monthly, or more frequently as the members of the JMC may determine in their reasonable discretion.

(iv) ***Responsibilities of the JMC.*** The responsibilities of the JMC are to:

(A) ensure that the marketing and onboarding interests of the parties are aligned;

(B) develop an annual joint marketing plan, including goals and targets, and budgets for approval by the JEC;

(C) agree on principles and practices for sharing information about the market and prospects;

(D) establish, and modify when appropriate, marketing and onboarding processes including the qualification of prospects, leveraging the Service Provider processes to the extent possible;

(E) establish, and modify when appropriate, standards for proposals, leveraging the Service Provider standards to the extent possible;

(F) monitor progress against tactical marketing and onboarding plans and activities ;

(G) ensure that the benefits of gainsharing are applied consistent with the terms of the contract;

(H) approve joint communications;

(I) approve and undertake major marketing events as appropriate;

(J) escalate issues to the JEC in the event of conflict or dispute;

(K) prepare annual progress reports on marketing and onboarding activities;

(L) monitor relationships with key stakeholders in the success of Hosting Solutions BC, including those stakeholders that deliver the Services;

(M) monitor the reputation of Hosting Solutions BC and its services.

3.3 **Joint Operations Committee (JOC).** The operations committee ("Joint Operations Committee" or "JOC") will function as the operational level governance body for the Agreement and for the provision of the Services to the Province under the Agreement. The JOC will have responsibility for the day-to-day relationship between the Province and the Service Provider and the delivery of the Services to the Province under the Agreement.

(a) ***Composition of the JOC.***

(i) Province: STMS AMO Lead

(ii) Service Provider: Service Provider STMS Lead

Other employees, consultants, or advisors of the Province and the Service Provider may attend meetings of the JOC at the invitation of either Party to the extent reasonably necessary to sufficiently address matters for discussion on the agenda of a JOC meeting. The JOC may also invite Buyers and industry and government leaders to participate in such meetings to facilitate information exchange and increase the value of the strategies discussed.

(b) ***Chair of the JOC.*** STMS AMO Lead

(c) ***Changes in Composition of the JOC.*** Each of the Parties may from time to time change its respective representatives on the JOC by providing written notice to the other Party of such change. Notwithstanding such right to replace individuals, the parties agree that such replacements

shall be of a similar or greater authority unless otherwise agreed by the other Party.

(d) ***Meetings of the JOC.*** The JOC shall hold meetings or telephone or video conferences at least monthly, or more frequently, as the members of the JOC may determine in their reasonable discretion.

(e) ***Special Meetings of the JOC.*** Notwithstanding the foregoing, the chair of the JOC may call a special meeting to consider any relevant issue upon reasonable prior notice to the other members of the JOC, such notice shall set forth the matters to be discussed or determined at such special meeting. A special meeting of the JOC, once called, shall be convened as soon as reasonably practical.

(f) ***Quorum.*** A quorum for any meeting of the JOC shall be one representative of each Party.

(g) ***Responsibilities of the JOC.*** The responsibilities of the JOC are to:

(i) prepare an Annual Operating Plan;

(ii) review the current status of the Annual Operating Plan;

(iii) manage the Change Order Process;

(iv) on an annual basis propose improvements and additions to the Service Levels;

(v) review the findings of benchmark or other studies as may be agreed to;

(vi) summarize and present findings to the JEC on any significant changes that need to be made to objectives, strategy, the Agreement, or the relationship between the Parties;

(vii) identify risks and barriers to success and ensure there are plan to mitigate;

(viii) identify and address and resolve any conflict escalated to it;

(ix) identify and manage impending change;

(x) continuously assess how the parties are working together, and plan steps to improve the relationships;

(xi) continuously look for new ways to deliver business value;

(xii) proactively seek advice on and sharing "best practices";

(xiii) make recommendations to the JEC and escalate issues that cannot be solved within current administrative practice;

(xiv) provide leadership by championing the objectives of the Agreement and identify any systemic contractual or management problems;

(xv) establish and manage the activities and results of permanent and ad hoc Joint Working Groups; and

(xvi) conduct annual review of reporting requirements set forth in **Schedule 21** (*Reporting Requirements*) of the Agreement.

(h) ***Dispute Resolution.*** In the event issues are raised which either or both parties do not consider have been appropriately addressed after reasonable efforts by the JOC, such issues may be escalated to the JEC.

3.4 **Joint Working Groups.** The following Joint Working Groups will commence as soon as practical after commencement of the agreement.

(A) Client Services (WTS) Working Group – governing principles to be determined by the Client Services (WTS) Working Group and approved by the JOC;

(B) Technology Architecture Working Group - governing principles as set forth in the attached Appendix A (Principles of the Technology Architecture Working Group);

(C) Privacy and Security (WTS) Working Group - governing principles to be determined by the Privacy and Security (WTS) Working Group and approved by the JOC; and

(D) Transformation Working Group - governing principles to be determined by the Transformation Working Group and approved by the JOC.

3.5 **Province Change Advisory Board.** The Service Provider will be invited to participate in the Province Change Advisory Board meetings to consider changes to the technical aspects of the Services or the delivery of the Services by the Service Provider to the Province, including, without limitation, Ordinary Course Changes contemplated in Section 7.1 and 7.2 (*Change Order Process*) of the Agreement.

4. **Meeting Protocols.**

The Parties acknowledge and agree that, to the extent possible, all governance meetings should follow the following standard business practices for meeting etiquette:

(a) to the extent possible, the governance committee will establish a pre-determined schedule of meeting dates, which will be communicated to the members by the chair;

(b) any unscheduled meeting dates, and changes to any scheduled or unscheduled meeting dates, will be communicated in writing (or by email) by the chair to the committee members at least five Business Days in advance, where possible, unless the five Business Day notice period is waived by all members of the committee, and except for unexpected or

emergency situations that do not permit such five Business Days notice period to be given; meetings shall start at the stated time on the circulated agenda;

(c) meetings shall start at the stated time on the circulated agenda;

(d) meeting invitees will indicate their ability to attend the meeting at least 3 Business Days prior to the meeting and, if unable to attend, to send an appropriate delegate with decision-making authority;

(e) where attendance of committee members is mandatory, meeting notices will indicate such mandatory attendance;

(f) any member of a committee may call a meeting of such member's committee outside of regularly scheduled meetings by sending a request to the chair of such committee that the meeting be called, and stating the purpose of the meeting and the details of the matters to be considered or discussed at the meeting;

(g) meeting agendas and meeting materials will be established by the committee chair and will be circulated by the chair to the committee members with as much prior notice as is reasonably possible, but in any event not less than 24 hours before any meeting;

(h) unless the meeting notice indicates that attendance must be in-person, to the extent possible the meetings of committees will be held in-person, provided that the members of a committee may hold their meetings by way of video conference, telephone conference or any other communication facility where all persons participating in the meeting can hear each other and make themselves heard; and

(i) minutes of all meetings of the committee will be taken by the chair of the committee or an individual appointed by the chair and circulated to all members of the committee as soon as practicable following the conclusion of a meeting but in any event, within five Business Days after the meeting. The members of the committee will have five Business Days to provide their comments on the minutes or object to the minutes by notifying the chair of such comments or objection, in writing. Where no comments or objection is received within the 5 business Day period, the minutes will be deemed to be accepted. The chair will circulate the final copy of all minutes of the meetings of the committee to the members on a timely basis.

APPENDIX A

PRINCIPLES OF THE TECHNOLOGY ARCHITECTURE WORKING GROUP

With respect to the Technology Architecture Working Group, the Parties acknowledge and agree to adhere to the following guiding principles when performing their activities:

1. The Province will develop and set the technical service architecture standards governing the Services provided to Province;

2. Service Provider will deliver the Services and Transformation Projects set forth in Schedule 9 (*Transformation SOW*) using the technology platforms agreed to by the Parties as of the Effective Date;

3. Service Provider will identify new or evolving hardware and software opportunities and prepare opportunity analyses that address Service impacts, benefits and costs;

4. The Province will identify Province requirements for new hosting services and will approve the introduction of new or evolved services prior to implementation of the new services;

5. Service Provider and the Province will work cooperatively and jointly to:

   - determine which new services should be considered;

   - determine enhancements to the current Services; and

   - develop orderly migration paths for new services and maintain hardware and software currency;

6. The Province will approve aspects of the architecture and design of the Services which directly affect the architecture, design or cost of the external Province IT infrastructure;

7. Service Provider will approve aspects of the internal architecture and design of the Services which do not directly affect the architecture, design or cost of the external Province It infrastructure; and

8. Service Provider will implement new services in accordance with the Change Order Process.

SCHEDULE 19

KEY POSITIONS

The following Service Provider positions are designated as Key Positions and are subject to the provisions of Article 11 of the Agreement:

Strategic Transformation and Mainframe Services (STMS) lead

Managed Services lead

Transition and Transformation lead

Security & Privacy lead

Business Continuity/ Disaster Recovery lead

Data Centre Lead

Mainframe Services Lead

The Province acknowledges that several of the Service Provider Key Positions shall initially be filled by individuals seconded from an Service Provider Affiliate, and that these individuals may be required to return to the Affiliate within 2 years of the Hand-Over Date.

With respect to the Service Provider Key Positions in Table 1 below, Service Provider shall use reasonable efforts to maintain the initial incumbent for the minimum initial periods of the Agreement from the Hand-Over Date specified in Table 1 (subject to the occurrence of any unforeseen events/circumstances). For greater clarification, after the expiry of such minimum initial period, any replacement appointments in any such Service Provider Key Positions shall not be required to remain in such Service Provider Key Position for any minimum period. Notwithstanding the foregoing Service Provider shall use reasonable efforts to maintain continuity in such positions as contemplated under Article 11 of the Agreement

Service Provider Key Position	Minimum Initial Period
Strategic Transformation and Mainframe Services (STMS) lead	18 months
Managed Services lead	18 months
Transition and Transformation lead	18 months
Security & Privacy lead	18 months
Business Continuity / Disaster Recovery lead	18 months
Data Centre Lead	24 months
Mainframe Services Lead	24 months

Table 1. Minimum Initial Periods for Service Provider Key Positions

SCHEDULE 20

SUBCONTRACTOR MATTERS

Material Subcontractors	Access Subcontractors

At issue for Inquiry

Any Subcontract entered into by the Service Provider for the performance of any part of the Services by a Subcontractor, where the Subcontractor has an annual dollar value from service of $1,500,000 or more in respect of the Services, shall constitute a "**Material Subcontract**" to which the provisions of Section 12.9 (*Additional Material Subcontract Terms*), in addition to the provisions set forth in Section 12.3 (*General Contract Terms* (*Subcontractors*)), shall apply, but excluding there from the following, none of which shall constitute "Material Subcontracts":

(a) Contracts with Suppliers;

(b) corporate personnel agencies who are Canadian Entities and whose External Personnel who may have access to Personal Information have signed External Personnel Agreements, and where such External Personnel do not use the Systems or premises of such corporate personnel agency in the performance of the Services but instead use those of some other Person and provided that all provisions of this Agreement relating to Systems and premises shall continue to apply with respect to the Systems and premises used by the External Personnel; and

(c) a Subcontract that is not a "Material Subcontract" when originally entered into, but through inadvertence subsequently has an annual dollar value in excess of the amount set forth above, provided that the Service Provider gives notice thereof to the Province as soon as possible through the Governance Process, and uses all reasonable efforts to subsequently cause such Material Subcontract to comply with the requirements of this Section.

SCHEDULE 21

REPORTING REQUIREMENTS

1. Purpose of Schedule.

This Schedule outlines the general reporting requirements for the Service Provider during the Term of the Agreement.

2. Definitions.

Capitalized terms used in this Schedule will have the meanings set forth in this Schedule 21 (*Reporting Requirements*) and capitalized terms not defined herein will have the meanings set forth in Schedule 1 to the Agreement.

3. General.

At all relevant times during the Term, the Service Provider will prepare or cause to be prepared and will provide to the Province in accordance with the provisions of this **Schedule 21** (*Reporting Requirements*) all reports and other deliverables as contemplated herein. The Service Provider will prepare and provide to the Province updates of such reports at such times as reasonably requested by the Province in accordance with the Change Order Process.

4. Guiding Principles to Reporting.

The Service Provider acknowledges and agrees that the Province expects the reporting and informational requirements of the Province under this Agreement will evolve during the Term, that reporting and informational requirements are intended to achieve the best value for reports to the Province in light of the circumstances applicable from time to time. Ordinary course changes to reporting and informational requirements, where the work effort for the Service Provider may be accommodated in the ordinary course of the Services, will not require a Change Request and will not increase the Fees; all other changes to the reporting and informational requirements will required a Change Request. In addition, the Service Provider will, from time to time, as the circumstances may render necessary or desirable, provide suggestions to the Province as to improvements, enhancements and changes to the reporting and informational requirements, for the Approval of the Province.

The Service Provider acknowledges and agrees that all planning, budgeting and reporting required pursuant to the terms of this Agreement will:

(a) be in accordance with any specific requirements as to timing, format and content set out herein;

(b) be timely, comprehensive and will contain accurate and complete information;

(c) contain such information as is reasonably necessary to allow the Province to fully monitor the Service Levels and the provision of the Services;

(d) be consistent with plans and budgets from time to time adopted by the Province; and

(e) updated from time to time as set forth in this **Schedule 21** (*Reporting Requirements*) and the Agreement (including, for greater certainty the Schedules to the Agreement).

5. Support for the Production of Province Reports.

The Service Provider will provide support to the Province for the Province's production of reports that are required to be delivered by the Ministry, internally within the Province. The Service Provider will support the gathering of the information for design and production of Province reports, up to sixty (60) man-hours per calendar quarter. The Province reports known at the Effective Date include the following:

(a) Office of the Comptroller General reporting obligations as set out in relevant policies standards including:

(i) *Financial Administrative Act* (British Columbia), and

(ii) *Core Policy Manual* (includes budgeting forecast requirements);

(b) *Auditor General Act* (British Columbia) reporting obligations as set out in relevant policies standards;

(c) privacy reporting obligations as set out in related legal, regulatory and policy (e.g., *Freedom of Information and Protection of Privacy Act* (British Columbia)) including:

(i) adherence to security standards,

(ii) freedom of information reporting requirements;

(d) CIO policies and standards;

(e) Risk Management Branch polices and standards;

(f) reporting on the success of the relationship and realization of benefits for the following:

(i) Treasury Board,

(ii) Cabinet,

(iii) Office of the Auditor General,

(iv) Office of the Comptroller General,

(v) the public,

(vi) the Ministry, and

(vii) the Joint Executive Committee.

6. Production of Standard Reports by Service Provider.

The Service Provider will provide reports as required:

(a) by the Agreement;

(b) by any statement of work contemplated under the Agreement;

(c) as set out in Table 1 below; and

(d) in conjunction with Service Level reporting.

7. Monthly Reporting – Performance.

With respect to the performance of the System in production, Service Provider will submit a standard set of reports to the Province by the tenth business day of each calendar month. This standard set of reports will consist of those reports identified in Section 9 as being produced monthly.

8. Monthly Reporting - Change Requests.

With respect to Change Requests (proposed, approved, active and resolved), the Service Provider will submit a report to the Province by the tenth business day of each calendar month. These reports will provide a status update in a format to be agreed to by the Parties and will reflect the progress, issues and resolutions relating to change requests active in the prior month.

9. Annual Operating Plan.

The Service Provider will, with the co-operation and assistance of the Province, prepare and provide to the Province the Annual Operating Plan in accordance with Sections 13.5 (*Annual Operating Plan*) to 13.7 (*Annual Confirmation*) of the Agreement.

10. Required Reports, Plans and Other Documentation

Table 1 – Reporting Requirements

To the extent the reports listed in the table below are produced by WTS as of the Effective Date, the Service Provider will produce such reports in a form substantially similar to the same reports produced by WTS prior to the Effective Date and at the frequency set forth in the table below.

Report Name	Report Contents	Frequency[1]
*Services Continuity Plan	A plan defining the steps required to recover one or more of the Services. The plan will also identify the triggers for invocation, people to be involved, communications etc. The Services Continuity Plan should be part of a Business Continuity Plan.	Annually, updated quarterly[2] or as material changes are made to Services.
Service Improvement Plan	A plan to implement improvements to a process or the Services.	Annually, updated quarterly or as material changes are made to Services.
*Root Cause	A report that summarizes the Service Provider's	As Problem is

[1] The date for the delivery of a report, plan, document, etc., under this Schedule 21 (*Reporting Requirements*) shall be ten (10) Business Days following the expiration of the date set forth under the column "Frequency" unless the Parties agree otherwise in writing.

[2] "quarter" or "quarterly" means the period of three (3) months ending on the last day of March, June, September or December in each calendar year.

Report Name	Report Contents	Frequency[1]
Analysis Report	assessment of the results of any root-cause analysis conducted for all Problems and includes a remediation plan for the error and a mitigation plan for avoiding the Problem in the future.	identified.
*Asset Register	Inventory of assets, including, a summary of changes made to the assets during the period.	Quarterly
*Asset Registry Changes	Summary of changes made to the assets during the period.	Monthly
*Service Outage Analysis Report	A report that identifies underlying causes of an unplanned Service interruption; includes the remediation actions taken for the outage and a mitigation plan for avoiding the outage in the future. The Service Outage Analysis Report identifies opportunities to improve the Service Provider's processes and tools, as well as the infrastructure.	As service outages are incurred.
*Incident Summary Report	A report containing a list of key information for all incidents recorded in the period including the status of each incident, monthly trends (total opened, total closed, month-to-month open, etc.) and the information required pursuant to the *Managed Services Statement of Work.*	Monthly
*Severity 1 and 2 Incident Report	A report containing a list of key information for all Severity 1 or Severity 2 incidents recorded in the period.	Weekly
*Outstanding Incident Report	A report containing a list of key information for all incidents outstanding as of the end of the period.	Monthly
*Problem/Known Error Report	A report containing the details of an outstanding Problem/known error or a Problem/known error that has been resolved and closed during the period.	Monthly
**Service Level Report	A report reporting achievement against Service Levels for the most-recent reporting period plus previous periods. A report containing details of one or more key performance indicators or other important targets that have exceeded or are forecast to exceed defined thresholds. Examples include SLA targets being missed or at risk to be missed, and a performance metric indicating a potential capacity Problem.	Monthly
*Security Incident Report	A report listing key information for all security incidents reported during the period.	Monthly
*Software Plan Change Report	A list of adaptive, corrective, preventative and perfective fixes undertaken for each application including date and time of correction, description of correction, corrective action taken, and root-cause analysis that is required.	Monthly

Report Name	Report Contents	Frequency[1]
*Hardware Plan Change Report	A list of adaptive, corrective, preventative and perfective fixes undertaken for each application including date and time of correction, description of correction, corrective action taken, and root-cause analysis that is required.	Monthly
*Capacity Plan	A Capacity Plan is used to manage the resources required to deliver the Services. The plan contains scenarios for different predictions of business demand, and costed options to deliver the agreed Service Levels.	Quarterly
*Capacity Utilization Report	Application usage, performance and database capacity report including capacity forecast based on historical trends and other known information.	Monthly
*Availability Plan	A schedule of planned system maintenance and planned outages.	Quarterly
*Change Plan	A plan that lists all requested or approved changes and their requested and planned implementation dates.	Weekly
*Projected Service Availability Report	A report that identifies the effect of planned changes on agreed Service Levels, based on the Change Plan.	Weekly
See SOWs	Reports as identified in or attached as an Appendix to the SOWs (and for greater certainty, including without limitation, SOW 2 – Data Centre Services, SOW 3 – Security Services, SOW 4 – Managed Mainframe Services, SOW 5A – Server Management Services, SOW 5B – Shared File and Print Services, SOW 5C – Web Hosting Services, SOW 5D – Virtual Hosting Services, SOW 5E – Onsite Support Services, SOW 5F – Citrix Based Computing Services, SOW 5G – Shared Database Services, SOW 5H – Application Enabling Services, SOW 6 – Storage and Backup Services, SOW 7 – Services Management Services, SOW 8 – Business Continuity and Disaster Recovery Services and Transformation SOW (see Schedule 9))	In accordance with the terms of the SOWs

* The Parties agree that during the Transformation Program (defined in the Transformation SOW), this report will be retired as new reports identified in the Statements of Work in Schedule 6 of the Agreement are introduced to replace them.

** The Parties agree that during the Transformation Program, this report will be retired as a new report identified in Schedule 11 of the Agreement is introduced to replace it.

SCHEDULE 22

RECORDS PROTOCOLS

This Schedule identifies the responsibilities among the Parties to meet the records management requirements set out in Article 14 (*Maintenance of Re*cords) of the Agreement.

With respect to Section 14.1 (*Maintenance of Records*) of the Agreement, physical Province Records that are transferred to, created by, or in the custody of the Service Provider will be managed in accordance with the Roles and Responsibilities Matrix below. From and after the Hand-Over Date, the Records that are identified in **Appendix A to Schedule 22** (*Records Protocols*), and that are transferred to, created by, or in the custody of the Service Provider will be managed in accordance with the Roles and Responsibilities Matrix below.

Further, any material amendments, modifications, or supplements to the practices and procedures identified in the Roles and Responsibilities Matrix below and impacting the Service Provider responsibilities under the Agreement including, to achieve compliance with respect to electronic records, shall be implemented in accordance with the Change Order Process.

Notwithstanding Section 14.1 of the Agreement, the Service Provider will maintain the following access,

S. 15

S. 15

	ROLES AND RESPONSIBILITIES	SERVICE PROVIDER	PROVINCE
1.	Establish Province-wide polices and standards for recorded information management practices.		X
2.	Establish standards for the development of ARCS and ORCS for all administrative records and operational records of the Province. (see: http://www.bcarchives.gov.bc.ca/arcs/index.htm)		X
3.	Establish standards for secure and confidential destruction of records; monitor records destruction operations; identify inadequate procedures or processes.		X
4.	Establish recorded information management program; designate a records officer responsible for administering the program, including the development and implementation of Ministry policies and procedures for recorded information management.		X
5.	Adopt and maintain recorded information management policies, including policies and procedures for the management of electronic records.		X
6.	Propose records retention schedules and recommend final dispositions in consultation with the Province's Corporate Records Management Branch.	X	
7.	Provide appropriate documentation for final dispositions of recorded information.		X
8.	Identify changes in the business process that may require the creation, addition or modification to Province records retention schedules.	X	
9.	Coordinate storage with records centres for semi-active records.	X	
10.	Establish records management processes responsibilities for Personnel and External Personnel (e.g., classifying documents according to established schedules).	X	
11.	Maintain active files of recorded information on-site; use appropriate labels to identify file descriptions and retention schedules.	X	
12.	Maintain records scheduled for return to the Province distinctly from those scheduled for off-site storage.	X	
13.	Box records in accordance with instructions from the Province for transfer to the Province designated Records Officer for review and approval.	X	

	ROLES AND RESPONSIBILITIES	SERVICE PROVIDER	PROVINCE
14.	Box records in accordance with disposition status, (e.g. "destruction", "selective" or "full" retention); prepare appropriate records management forms for transfer to off-site facilities; send completed forms documentation to the Province designated Records Officer for review and approval.		X
15.	Review submitted forms; forward as required approved forms to the Province's Corporate Records Management Branch for processing; return completed approved forms. Update access authorizations for boxes in off-site storage.		X
16.	Schedule transfer of records to off-site storage; pick-up boxed records.		X
17.	For retrieval of records from off-site storage: authorized person contacts off-site facility; storage company delivers records.	X	
18.	Retention and disposal of inactive records in off-site storage according to appropriate schedules.		X
19.	Secure disposal on-site of records not sent to off-site storage if approved in accordance with the process set forth in item number 15 above.	X	
21.	Litigation Coordinator – coordinate between Crown Counsel, Ministry of Labour and Citizens' Services and the Service Provider regarding litigation actions.		X
22.	Provide Service Provider training regarding recorded information management, new policies and procedures.	**X**	
23.	Provide training to Service Provider trainers regarding recorded information management, new policies and procedures.		**X**
24.	Representative on Ministry Records Officer Council, ARCS Review Committee and other cross-government committees or meetings related to records management policy and procedures.		X

APPENDIX A

1. RECORDS TRANSFERRED TO THE SERVICE PROVIDER

1.1 Disaster Recovery Plans. All Province disaster recovery plans provided to the Service Provider prior to the Hand-Over Date.

1.2 Capacity Planning and Trending. Province capacity planning and trending for the three server groups:

(a) Open VMS - tool (Command Central);

(b) Windows - trend documents for shared file and print only (rolled up into one year reports); and

(c) Open Systems – snapshot information.

1.3 Service Profiles/Service Descriptions.

(a) Service Descriptions;

(b) Status of Work in Process Projects; and

(c) Explicit Agreements.

1.4 Asset Inventories. Asset inventory lists including equipment, hardware and software used in connection with the Services provided at the Province Data Centres, the Regional Network Centres and the Remote Sites.

1.5 Windows Server Install Records. Province server configuration details.

2. RECORDS CREATED BY THE SERVICE PROVIDER FROM AND AFTER THE HAND-OVER DATE

2.1 Disaster Recovery Plans. The Service Provider will create specific disaster recovery plans for:

(a) enhancements to the Province's disaster recovery plans;

(b) the Services being performed at the STMS Data Centre; and

(c) Ministry Clients as requested by them as part of the optional Services.

2.2 Capacity Planning and Trending. Province capacity planning and trending for all servers and the mainframe.

2.3 Service Profiles/Service Descriptions.

(a) Statements of Work;

(b) Services Catalogue;

(c) the Manual; and

(d) any other manuals referred to in the SOWs.

2.4. Asset Inventory Lists. Monthly asset inventory lists including equipment, hardware and software used in connection with the Services after the Hand-Over Date.

2.5 System and Security Logs from the Supported Infrastructure. The Service Provider will provide log information in accordance with the provisions of the Security SOW.

2.6 Server Install Records. Server configurations as described in the Midrange SOWs (as defined in Schedule 23 (*Fees*)).

3. SYSTEMS THAT PRODUCE RECORDS

3.1 Information Technology Incident Management System (ITIMS)

- Records of incident and problem diagnosis and resolution (break and fix data), and Records produced from the Change Management Process – to the extent records are transferred to, created by, or in the custody of the Service Provider (including records produced through ITIMS).

3.2 Digital Workflow – records supporting billing (including records received form the Province's Remedy System.

3.3 Service Provider Billing System

- Monthly invoices.
- Records supporting billing (excluding Digital Workflow covered above).

3.4 STMS Data Centre

- Power consumption reports.
- STMS Data Centre physical access logs.
- STMS Data Centre video logs.

3.5 SOW Records

- Any other Records referred to in the SOWs.

SCHEDULE 23

1. OVERVIEW

1.1 Terms

Capitalized terms used in this Schedule without definition have the meanings attached to such terms in the Agreement. Article 11 (*Definitions*) below contains a list of definitions or terms defined elsewhere in this Schedule.

1.2 Summary

This Schedule 23 contains all the Fees payable by the Province to the Service Provider for delivery of Services under the Agreement, including the fees for the Managed Services and the Data Centre Services provided under the Agreement.

1.3 Appendices

The following Appendices are attached to this Schedule:

Appendix A (*VA Price Tables*)

Appendix B (*STMS Data Centre Price Table*)

Appendix C (*Managed Services Price Table*)

Appendix D (*Volume Band Adjustments*)

Appendix E (*BC CPI and Data Centre CPI Instructions*)

Appendix F (*Pro-Ration of Margin Cap For Annual Growth*)

Appendix G (*Margin Cap Example And Margin Cap Adjustments*)

Appendix H (*Optional Security Services*)

Appendix I (*Transformation Deliverables (with Transformation Fees)*)

Appendix J (*Services Catalogue*)

Appendix K (*Intentionally Left Blank*)

Appendix L (*Intentionally Left Blank*)

Appendix M (*Hourly Rates*)

Appendix N (*Termination Services Time And Material Rates*)

1.4 Currency

All amounts in this Schedule 23 are in Canadian dollars unless otherwise stated.

2. UNIT PRICES

2.1 Overview

The pricing tables attached as Appendix C (the "**Managed Services Price Table**") include unit pricing that applies in each Contract Year of the Initial Term based upon the SOWs. A "**Unit Price**" is a monthly price, and where indicated is a one-time price, for a service unit within each category of the Managed Services Price Table.

The Managed Services Price Table is adjusted each Contract Year in accordance with Section 6.3 (*Managed Services Inflation*) below; and the Unit Price's will be adjusted as required in accordance with Section 3 (*Volumes and Volume Banding*) below.

Table 1 below contains a summary of the various types of Unit Prices found in the Managed Services Price Table .

Table 1 - Summary of Managed Services Unit Prices

Area	Category	Basis for Unit Price
Midrange Services	Midrange physical Management	Per Server per month
	Midrange physical Hardware and Software and Software Maintenance	Per Server per month or per Server one-time
	Midrange Virtual Hosting Services	Per virtual Server per month
	Portion of Host Server Support and Host Service Hardware	Per virtual Server per month
	Shared services (Shared File Print, Shared Web, Shared Database)	Various per month (e.g. per user for SFP, per instance for Shared Database, per site for Shared Web)
	Other midrange services (Citrix, Middleware, Server Installation)	Various per month or one-time (e.g. per Server, per instance, per install)
	Optional Midrange Services	Per Server per month
Managed Mainframe Services	Mainframe Processing	Per MIP per month
	Non-standard software (WHS)	Monthly fee
	DASD	Per GB per month
	Tape	Per GB per month
	Hardware	Per unit one time
	Optional mainframe services	Various per month or one-time)

Area	Category	Basis for Unit Price
Managed Storage and Backup Services	Province Owned Equipment	
	Managed Storage	Per GB per month
	Managed Backup	Per GB per month
	Extended Retention	Per GB per month
	Service Provider Owned Equipment	
	Managed Storage	Per GB per month
	Managed Backup	Per GB per month
	Extended Retention	Per GB per month
	Hardware	Per unit one time
	Optional Storage Services	Various (e.g. per GB per month, hardware one-time)

2.2 Midrange Services

The following provides additional information on the characteristics of the various midrange Unit Prices, which are all monthly prices, unless otherwise indicated. The Services to which these Unit Prices apply are more particularly described in the following SOWs (collectively, the "**Midrange SOWs**"):

- SOW 5A - Server Management Services
- SOW 5B - Shared File and Print Services
- SOW 5C - Web Hosting Services
- SOW 5D - Virtual Hosting Services
- SOW 5E - Onsite Support Services
- SOW 5F - Citrix Based Computing Services
- SOW 5G - Shared Database Services
- SOW 5H - Application Enabling Services

2.2.1 Midrange Server Management Services

The Unit Price for the Server Management Services of a physical Server is based upon the different types of physical Servers and Operating Systems, as set forth below:

Production Servers:

- Application Server – Server that operates Applications in support of Province business processes. For example, Province owned/licensed and operated custom developed or COTS based Applications (such as MS Exchange, ERP applications, HealthNet, Citrix, Sharepoint);

- Database Server – Server that operates a Province Database Management System (DBMS) (such as Oracle, SQL Server);

- Web Hosting Server – Server that runs a web engine for a Province websites (such as Apache, Tomcat and IIS);

- Infrastructure Server – Server that does not require Applications, such as Active Directory, File Transfer Protocol (FTP) Servers. Infrastructure Servers do not run Province-facing applications, but run services that allow Province-facing and other applications to operate.

Development / Test Servers:

- Development / Test Server – Server that is used solely for developing and testing purposes and is not used for in the production environment. Any of the Servers referred to above may have an associated development/test Server.

2.2.2 Server Tiers

The physical Servers have been categorized into Tiers as set out below. For Virtual Servers, there are no Tiers as the Virtual Servers are offered at the equivalent of a Tier 2 level (with available optional services as described in the Managed Services Price Table. The Tier depends on the services provided and the Server location.

- Tier 1
  - Available as a cluster within a single Province Data Centre or STMS Data Centre
  - 7x24 support
  - Cluster Management - Requires at least two Servers

- Tier 2
  - Single hosted Server
  - Province Data Centre or STMS Data Centre locations only
  - 5x9 support
  - 3 month commitment on Virtual Servers
  - There are different support hours Unit Price options available: 5x12, 7x24

- Tier 3
  - Single hosted Server
  - Remote locations and Regional Network Centre (non-Data Centre locations)
  - 5x9 support
  - There is an optional Unit Price for 7x24 support hours

2.2.3 Midrange Physical Hardware and Software

Refer to Section 2.7 (*Hardware*) below for the treatment of hardware.

The hardware Unit Price in the Managed Services Price Table is based upon the hardware configurations described in the SOWs. Any upgrades to these configurations that are requested

by the Province (such as additional RAM or hard drives) are on a time and materials basis using the Service Provider's Hourly Rates.

The software Unit Price in the Managed Services Price Table is based upon software for which the Service Provider is responsible on the Service Provider Owned hardware.

2.2.4 Midrange Virtual Hosting Services

The Unit Price for the Virtual Hosting Services of a Virtual Server is based upon the type of the Virtual Server and its Operating System. There are Unit Prices for the following types of Virtual Servers:

- Application Server
- Database Server
- Web Hosting Server
- Infrastructure Server
- Development / Test Server

The description of the different types of Virtual Servers is the same as set forth above in Section 2.2.1(*Midrange Server Management Services*) for a physical Server.

2.2.5 Host Server Support

Each Virtual Server is charged a portion of the cost of the Host Server support for the physical Host Server on which it resides, by way of a separate monthly Unit Price, as more particularly set forth in Managed Services Price Table.

2.2.6 Host Server Hardware At issue for Inquiry

Each Virtual Server is charged a portion of the cost of the Host Server hardware on which it resides where the total cost of the physical Host Server is less than by way of a separate monthly Unit Price, as more particularly set forth in Managed Services Price Table.

2.2.7 Host Server Hardware At issue for Inquiry

Where the total cost of the physical Host Server is more than then:

(a) except as set forth in paragraph (b) below, the cost of a physical Host Server will be paid for by the Province as a one-time Unit Price, as more particularly set forth in Managed Services Price Table, to be paid by the Province to the Service Provider in the manner described in Section 2.7 (*Hardware*) below;

(b) the number of Host Servers included in the Capital Payment for any Contract Year will be based upon the number of Virtual Servers and the "Virtual Ratios" as set forth in SOW 5D (*Virtual Hosting Services*); and

(c) if the Service Provider does not meet the Virtual Ratios and is required to purchase an additional Host Server (the "**Extra Host**"), then the Service Provider will fund the cost of the Extra Host and will not charge the cost of the Extra Host to the Province;

(d) if in any following Contract Year:

(i) the Service Provider exceeds the Virtual Ratios and does not require all of the Capital Payment Estimate to purchase Host Servers in that Contract Year, then

(ii) the Service Provider may use that Contract Year's Capital Payment to pay for the remaining value of the Extra Hosts bought in a prior year, where the remaining value is the Unit Price of the Extra Host pro-rated for the remaining life of the Extra Host.

2.3 Midrange Shared Services

2.3.1 Shared File and Print Services

The Shared File and Print Services (SFP) Unit Price is a monthly per user fee for access to the Shared File and Print Services and includes the support of the SFP environment, hardware associated with the environment (other than storage, back-up and retention hardware), and support for storage, backup and retention for each user based upon 1.5 GB of allocated Tier 2 storage per month, as more particularly described in Schedule 5B (*Shared File and Print SOW*) (the "**SFP Base Unit Price**").

Where a Client Ministry exceeds the 1.5 GBs per user per month of storage calculated on an aggregate basis for all of the SFP users in the Client Ministry, a Unit Price for additional SFP GBs (that covers the same elements as listed above for the SFP Base Unit Price) will apply as per the Managed Services Price Table (the "**SFP Incremental Unit Price**"). The Fees for the additional SFP GBs of storage used by the Client Ministry, in the aggregate in any one month, will be based upon SFP Incremental Unit Price and will be calculated as follows:

(a) actual aggregate Tier 2 SFP storage volumes measured in GBs for the Client Ministry;

(b) less an amount equal to 1.5 GBs multiplied by the number of SFP users in the Client Ministry (being the 1.5 GBs per user that are covered under the SFP Base Unit Price); and

(c) where (a) less (b) is a positive number, then such positive number multiplied by the SFP Incremental Unit Price; or

(d) where (a) less (b) is negative number, the SFP Incremental Unit Price does not apply, and accordingly, only the SFP Base Unit Price will apply.

As described in the Schedule 9 (*Transformation SOW*), the SFP Base Unit Price includes a Transformation of the Province's current SFP environment. The Unit Price also includes the operational benefit of the project via reduced monthly Unit Prices.

2.3.2 Shared Database Services

The monthly Unit Price for the Shared Database Services is based upon a Shared Database. and includes the support of the Shared Database environment, hardware associated with the environment (other than storage, backup and retention hardware), and support for storage, backup and retention for each Shared Database based upon 5 GBs of allocated Tier 2 storage per month. The Shared Database Services are as more particularly described in Schedule 5G (*Shared Database Services SOW*).

If a Shared Database requires more than 5 GBs of Tier 2 storage per month, then additional GBs of Tier 2 storage may be purchased in increments of 1.0 GBs for a Unit Price (that covers the same elements as listed above for the monthly Unit Price) as set forth in Managed Services Price Table.

2.3.3 Shared Web Hosting Services

The monthly Unit Price for the Shared Web Hosting Services is based upon a website hosted on a Shared Web Hosting Server, and includes the support of the Shared Web Hosting Server environment, hardware associated with the environment (other than storage, backup and retention hardware), and support for storage, backup and retention for each website on the Shared Web Hosting Server based upon 0.5 GBs of allocated Tier 2 storage per month. The Shared Web Hosting Services are as more particularly described in Schedule 5C (*Web Hosting Services SOW*).

If a website on a Shared Web Hosting Server requires more than 0.5 GBs of Tier 2 storage per month, then additional GBs of Tier 2 storage may be purchased in increments of 0.5 GBs for a Unit Price (that covers the same elements as listed above for the monthly Unit Price) as set forth in the Managed Services Price Table. .

2.3.4 Initial Server Installations

The one-time Unit Price for the installation and setup of a Server (including a physical Host Server) or a Virtual Server applies; (i) for the replacement of Province Owned Equipment with Service Provider Owned Equipment, (ii) new Service Provider Owned Equipment that is purchased for a net new purpose other than a Server refresh referred to in Section 2.3.5 (*Refresh Server Install*) below; and (iii) a Virtual Server that is hosted on a Host Server under (i) or (ii). The one-time Unit Prices are as set forth in the Managed Services Price Table and are based upon the following types of Servers, Host Servers and Virtual Servers:

Servers and Host Servers

- Wintel and Linux
- Solaris and AIX
- Open VMS

Virtual Server

- VMWare (Window and Linux)
- Solaris (Solaris and AIX)

2.3.5 Refresh Server Installations

The one-time Unit Price for the refresh installation and setup of a Server (including a physical Host Server) or a Virtual Server applies for the replacement of Service Provider Owned Equipment with new Service Provider Owned Equipment for refresh purposes. The one-time Unit Prices are as set forth in the Managed Services Price Table and are based upon the following types of Servers, Host Servers and Virtual Servers:

Servers and Host Servers

- Wintel and Linux
- Solaris and AIX
- Open VMS

Virtual Server

- VMWare (Window and Linux)
- Solaris (Solaris and AIX)

2.3.6 Citrix Server Support

The monthly Unit Price for Citrix Based Computing Services (as described in Schedule 5F (*Citrix Based Computing SOW*)) applies to the LOB Application Servers on a per Server basis and is in addition to the monthly Unit Price under Section 2.2.1 (*Midrange Server Management Services*). This Unit Price is set forth in the Managed Services Price Table.

For greater clarification, the monthly Unit Price for Citrix Based Computing Services does not apply to the Citrix Infrastructure Servers, but the monthly Unit Price under Section 2.2.1 (*Midrange Server Management Services*) for Application Servers does apply to the Citrix Infrastructure Servers on a per Server basis.

2.3.7 Dedicated Web Services – Optional

The monthly Unit Price for the optional Dedicated Web Services (as described in Schedule 5C (*Web Hosting Services*)) is based upon the web hosting software (Apache, Tomcat and IIS) that is used on the Dedicated Application Server, or on a Dedicated Application Server operating as a Virtual Server, as set forth in the Managed Services Price Table. For greater clarification, the Dedicated Web Services apply in addition to the monthly Unit Price under Section 2.2.1 (*Midrange Server Management Services*) or Section 2.2.4 (*Midrange Virtual Hosting Services*) as applicable.

2.3.8 Optional Midrange Services

Various optional midrange Services (the "**Optional Midrange Services**"), as more particularly described in the Midrange SOWs, may be purchased in connection with a Server or a Virtual Server. The monthly Unit Prices for the Optional Midrange Services are based upon the type of Server or Virtual Server (Wintel/Linux or Solaris/AIX):

- Applications Monitoring Services
- Batch Monitoring Services
- Database Management Services
- Cluster Management
- Image Performance Management
- Server Capacity (planning)
- Extended Support Hours - 5 x 12
- Extended Support Hours - 7 x 24
- Extended Support Hours - remote field services - 7 x 24

The Extended Support Hour services are the only Optional Midrange Services that are subject to minimum volume requirements, as described more fully in Section 3 (*Volumes and Volume Banding*) below.

Batch Scheduling and DR Recovery Plan/Test are other Optional Midrange Services available to the Province. The Unit Price for each of these other Optional Midrange Services is dependent upon the environment in which the optional service is performed and will be determined at the time the optional service is requested by the Province. For example, the Batch Scheduling Unit Price is dependent upon the number and frequency of batch jobs scheduled, the Application to which the batch job applies, and so on. A request for Batch Scheduling or DR Recovery Plan/Test will be made through the Province Ordering System.

2.3.9 Retiring Platforms (HPUX and Tru64)

The Managed Services Price Table provides Unit Prices for the following Operating Systems: Windows, Linux, Unix, Solaris, AIX and Open VMS. The Province is in the process of retiring HPUX and Tru64 Operating Systems (the "**Retiring Platforms**") by transitioning the Applications on the Retiring Platforms to a supported Operating Systems as listed above. The Parties expect that some of the Retiring Systems will still be in operation at the Hand-Over Date. The Parties acknowledge that Service Provider does not have Unit Prices for the Retiring

Platforms, or for transitioning the Applications from a Retiring Platform to a supported Operating System..

The Service Provider will support the Retiring Platforms based upon the Unix Server Management Services "small" Unit Price in the Managed Services Price Table. In the event the Service Provider cannot support the Retiring Platform in a similar manner as the Unix Server (for example, if a different monitoring agents or management tools are required), then the Service Provider will submit a Change Order to the Province for the additional cost to support the Retiring Platforms.

2.4 Managed Mainframe Services

Set forth below are the descriptions of the Unit Prices for the Mainframe Services and Optional Mainframe Services comprising the Managed Mainframe Service, all of which are more particularly described in Schedule 4 (*Managed Mainframe Services SOW*). The Unit Prices for the Managed Mainframe Services are all monthly charges unless otherwise indicated.

2.4.1 Managed Mainframe Services - Start Date

The Mainframe Services are expected to start on Until that date, Service Provider will not provide any Managed Mainframe Services or charge the Province for the Managed Mainframe Services, other than charges for the Mainframe Services Migration Project (as described more fully in Schedule 9 (*Transformation SOW*)) that are provided by the Service Provider to the Province prior to The Managed Services Price Table for the Managed Mainframe Services will be adjusted by inflation on in accordance with Section 6.3.5 (*BC CPI Inflation*) below.

At issue for Inquiry

If there are changes to the Managed Mainframe Services prior to their commencement on then the Parties acknowledge that there may also be a related changes to the Managed Services Price Table for the Managed Mainframe Services, all of which will be made through the Change Order Process.

2.4.2 Mainframe Processing

The Unit Price for Mainframe Services (other than for Non-Standard Software, DASD, Tape and hardware costs as discussed below) is charged on a per MIPS basis for the aggregate installed volume of MIPS per month (and for greater clarification, the Province will be charged for the total installed volume of MIPS per month regardless of its actual MIPS usage).

2.4.3 Non-Standard Software

The monthly Unit Price for the Non-Standard Software and related support is set forth in the Managed Services Price Table. Each Party is responsible for the ongoing license fees and maintenance support fees to the applicable third party software vendors for the Non-Standard Software for which each Party is the licensor (as set forth in Appendix D.2 (*Non-Standard Software*) attached to Schedule 4 (*Managed Mainframe Services SOW*)).

The Use Rights granted to Service Provider under the Master Transfer Agreement for the Non-Standard Software licensed to the Province are at no charge to Service Provider.

Any increases or decreases to the Unit Price for the Non-Standard Software will be made through the Change Order Process and pursuant to the Mainframe Software Plan to address the following:

(a) the addition or removal of Non-Standard Software used to provide the Managed Mainframe Services; and

(b) increases or decreases to the license or maintenance fees paid to third party vendors for the Non-Standard Software licensed to the Service Provider.

For greater clarification, the Unit Price for the Non-Standard Software will not be increased for inflation under the provisions of Section 6.3 (*Managed Services Inflation*) below.

2.4.4 DASD

The Unit Price for Direct Access Storage Device (DASD) services (excluding hardware costs) is charged on a per GB basis for the aggregate installed GBs for DASD per month (and for greater clarification, the Province will be charged for the total installed GBs for DASD per month regardless of its actual GB usage). The Unit Price for DASD is set forth in the Managed Services Price Table.

2.4.5 Tape

The Unit Price for the tape storage services (excluding hardware costs) provided under the Mainframe Services is charged on a per GB basis for the actual GBs of tape storage used per month. The Unit Price for the tape storage is set forth in the Managed Services Price Table.

2.4.6 Mainframe Hardware

The Unit Prices for the hardware associated with the Mainframe Processing, DASD and tape services are one-time costs for the initial hardware, as more particularly described in Section 2.7 (*Hardware*) below.

Any increases to the DASD or the tape storage required by the Province will be made through the Change order Process, based upon the following:

(a) increases from the initial DASD volume of 3,525 GBs, which may be increased by increments of 250 GBs at a cost of approximately for each 250 GB increment; and

At issue for Inquiry

(b) significant increases from the initial tape storage volume of 145,000 GBs, which will be determined at the time the change is requested (such as doubling the volume of tape storage which is at a cost of approximately).

2.4.7 Optional Mainframe Services

The Unit Prices for the different Optional Mainframe Services are either one-time, monthly or hourly fees as described below and as more particularly set forth in the Managed Services Price Table:

Monthly Unit Price

- Form/Print/end user Support – monthly fixed fee based upon the level of support as described in the Managed Mainframe Services SOW, subject to a minimum 12 month subscription for this Optional Mainframe Service.

One-Time Unit Prices

- SAS 70 Audit – A per occurrence fee for conducting a SAS 70 Audit of the mainframe.
- Extra DR Test – A per occurrence fee for conducting an extra disaster recovery test of the mainframe.

Hourly Unit Prices

- Database Administration – hourly rate based on a minimum of one day's support (8 hours).
- Database Production Support – hourly rate based on a minimum of one day's support (8 hours).
- Database Consulting Services – hourly rate based on a minimum of one day's support (8 hours).
    - The hourly rates are consulting rates and will be calculated every two years for inflation and market conditions.
    - The hourly rate do not include the following:
        - Project Management
        - Hardware specific to a project (the rate does include the Service Provider Personnel's PC and MS office suite used to provide the consulting services)
        - Special requirements of a project
        - Travel and living expenses

2.4.8 BC Mail Plus support

The Parties agree Service Provider will not support the BC Mail Plus requirements delivered pre-Service Provider contract by the current service provider of mainframe services.

2.5 Managed Storage and Managed Backup Services

Set forth below are the descriptions of the Unit Prices for the Managed Storage Services, the Managed Backup and Restore Services, the Extended Retention Services and other optional services comprising the Managed Storage and Managed Backup Services, all of which services are more particularly described in Schedule 6 (*Managed Storage and Managed Backup Services SOW*). The Unit Prices for the Managed Storage and Managed Backup Services are all monthly charges as set forth in the Managed Services Price Table, and such Unit Prices:

(a) exclude hardware, software and installation costs (see Section 2.7 (*Hardware*) below for the treatment of hardware associated with the Managed Storage and Managed Backup Services); and

(b) in the case of Extended Retention Unit Price for the Province Owned Equipment, includes tape media.

2.5.1 Managed Storage (Tier 1, 2, 3, and NAS)

The Unit Price for Managed Storage Services is charged differently in respect of the Province Owned Equipment and the Service Provider Owned Equipment, and is also charged differently for each particular Tier of service purchased, as described below. The Unit Price for Managed Storage Services does not apply to the storage in support of the "Midrange Shared Services" which is addressed separately in Section 2.3 (*Midrange Shared Services*) above.

The Managed Storage Services Unit Price for both the Province Owned Equipment and the Service Provider Owned Equipment is based upon a GB allocation requested by Client Ministries through the Province Ordering System, where the requested GB storage allocation is reserved for a particular Server or Network Attached Storage (NAS) and is charged based upon the allocation (regardless of actual use of that allocation). Increases to a particular GB storage allocation may be purchased in increments of 50 GBs through the Province Ordering System, other than for GBs for "NAS" which may be purchased in increments of 20 GBs.

- Tier 1 – is a class of disk storage that is the highest performing, highest availability and is designed with the most redundancy.

- Tier 2 – is a class of disk storage that has medium performing, high availability and is designed with a high level of redundancy.

- Tier 3 – is a class of disk storage that has an economy performing disk, lower availability than Tier 2 Service and is designed with a high level of redundancy.

- NAS –is file-level computer data storage connected to an IP network providing data access to heterogeneous network clients.

2.5.2 Managed Backup and Restore Services

The Unit Price for Managed Backup and Restore Services is charged differently in respect of the Province Owned Equipment and the Service Provider Owned Equipment. The Unit Price for Managed Backup and Restore does not apply to the backup in support of the "Midrange Shared Services" which is addressed separately in Section 2.3 (*Midrange Shared Services*) above, and is charged based upon the GBs actually used each month in performing the services.

2.5.3 Extended Retention Services

The Unit Price for Extended Retention Services is charged differently in respect of the Province Owned Equipment and the Service Provider Owned Equipment. The Unit Price for Extended Retention Services does not apply to the retention in support of the "Midrange Shared Services" which is addressed separately in Section 2.3 (*Midrange Shared Services*) above, and is charged based upon the GBs actually used each month in performing the services.

2.5.4 Optional Storage Services

The Unit Prices for the following Optional Storage Services are all monthly charges as set forth in the Managed Services Price Table, and such Unit Prices exclude hardware, software and installation costs (see Section 2.7 (*Hardware*) below for the treatment of hardware associated with the Managed Storage and Managed Backup Services):

- Tier 1, Mirrored Primary.
- Tier 1, with Local Clone Services, Mirrored Primary – Available when the STMS Calgary Data Centre is available.
- Tier 1, with Local Clone Services, at Same Site - Standard –Available when the STMS Calgary Data Centre is available.
- Tier 1, with Replication Services and Local Clone Services, Mirrored Primary – Available when both of the STMS Data Centres are available.
- Tier 1, with Replication Services and Local Clone Services, Standard – Available when both of the STMS Data Centres are available.
- Tier 2, Mirrored Primary.
- Tier 1, with Replication Services, Standard – Available when both of the STMS Data Centres are available.
- Tier 1, with Replications Services, Mirrored Primary – Available when both of the STMS Data Centres are available.
- Archive Storage Repository – Available when both of the STMS Data Centres are available (may be purchased without FSA described below).

- Files System Archive (FSA) – Available when both of the STMS Data Centres are available (may only be purchased when an equal amount of Archive Storage Repository described above is also purchased).

- VTL Backup to Encrypted Offsite Tape Service – Available when the STMS Calgary Data Centres are available.

The Tier 1 and Tier 2 Optional Storage Services listed above can be requested by the Client Ministries through the Province Ordering System, where the requested storage is charged based upon the allocation (regardless of actual use of the storage). The storage may be on an aggregate basis, or individually, depending upon the Optional Storage Service, as more particularly described in Section 3 *(Volumes and Volume Banding*) below.

2.6 Service Delivery Ops and Governance

The Service Delivery Ops and Governance (SDO&G) is included as a component in several of the Unit Prices in the Managed Services Price Table, and is indicated in each Unit Price where it is so included. The SDO&G includes the following:

- Management and operations support.

- Office space.

- Network;

  Network support and hardware less than (where network hardware greater than is part of the Capital Payment) and the network circuits are provided by the Province.

At issue for Inquiry

- Tool and Lab Servers:

  Service Provider has a number of tool and lab Servers that support the Managed Services.

- S15 as described in the Schedule 3 (*Security SOW*), which will be available when the STMS Data Centres are available for use in the Managed Services.

- BC Hydro rebate (see Section 5.6 (*BC Hydro Rebate*) below for more details).

Changes to the SDO&G component of the Unit Price will be addressed through the Volume Banding or through the Change Order Process, as applicable.

2.7 Hardware

Set forth below is a description of the treatment of hardware, and in the case of storage, backup and retention also software and installation by the Service Provider in providing the Managed Services under the Agreement. There are no charges for hardware where the Managed Services are delivered using Province Owned Equipment. Charges for hardware will commence upon the earlier of the refresh of existing Province Owned Equipment and the purchase of Service

Provider Owned Equipment for a net new purpose. The hardware, and also the software and installation for storage, backup and retention, will be charged to the Province in the following two ways:

(a) as a capital payment made by the Province to the Service Provider in of each Contract Year, as more particularly described in Section 2.7.1 (*Capital Payment*) below (the "**Capital Payment**"); or

(b) as a monthly Unit Price for hardware.

Hardware cannot be purchased as a stand-alone item without any associated Managed Services to be provided by the Service Provider.

2.7.1 Capital Payment

At issue for Inquiry

The Province will make a Capital Payment to Service Provider in of each Contract Year based upon the estimated capital requirements for the following as determined by the Parties each year in the Annual Operating Plan (each a "**Capital Payment Estimate**"), except that for the 2009 Capital Payment the Capital Estimate will be the capital amount set forth in the Managed Services Price Table for 2009/10, which does not include any growth for that period. The Service Provider will use the Capital Payment to purchase the following for use in delivery of the Managed Services:

(a) network hardware greater than At issue for Inquiry

(b) Server hardware greater than (excluding Service Provider tool Servers);

(c) mainframe hardware (processors, DASD and tape);

(d) storage, backup and retention hardware, software and installation (including for Optional Storage Services).

2.7.2 Annual Planning Process

As part of the Annual Operating Plan process, referenced in Section 13.5 of the Agreement, the Parties will update the capital amount set forth in the Managed Services Price Table for the applicable Contract Year to determine the following year's Capital Payment Estimate based upon:

(a) procurement plan for the hardware covered under the Capital Payment which includes the refresh plan, and growth for Servers, storage, mainframe and network hardware;

(b) the Server and storage hardware Unit Price from the Managed Services Price Table for the applicable Contract Year; and

(c) the mainframe and network capital amounts from the Managed Services Price Table.

2.7.3 Tracking of Capital Payment

Service Provider will track the application of the Capital Payment against capital purchases for hardware listed in Section 2.7.1 (*Capital Payment*) above (the "**Capital Purchases**") and report to the Province on a quarterly basis detailing the assets the Capital Payment funded.

The quarterly Capital Payment tracking will include a projection of the capital assets that are still to be purchased during the remainder of the Contract Year, and will compare the projections for the capital assets still to be purchased with the remaining Capital Payment for that Contract Year to forecast whether a surplus or shortfall is expected.

2.7.4 Treatment of Capital Payment Surplus or Shortfall

Where the Capital Payment less the amount of the Capital Purchases for any Contract Year is greater than zero (the "**Capital Payment Surplus**"), then the amount of the Capital Payment Surplus will be applied against the next Contract Year's Capital Payment, and will therefore reduce the amount of the Capital Payment to be paid to Service Provider in the next Contract Year.

Where the Capital Payment less the Capital Purchases (or planned Capital Purchases) for any Contract Year is less than zero (or expected to become less than zero) at any point before the expiry of the Contract Year (the "**Capital Payment Shortfall**"), then the Parties will work together through the Governance Process to determine a revised plan that addresses the Capital Payment Shortfall by one or both of the following:

(a) slowing down the planed Capital Purchases for that Contract Year to stay within the amount of the Capital Payment; or

(b) increasing the amount of the Capital Payment for that Contract Year (if approved by the Province).

2.7.5 Inability for Province to Fund Capital Payment

If the Province is unable to fund the Capital Payment, then all future equipment that would have been the subject of a Capital Purchase (the "**Future Hardware Purchases**") will be charged to the Province based upon a monthly hardware Unit Price, in which case, the annual Capital Payments referred to above will cease and be replaced with the monthly hardware Unit Price. The hardware Unit Price will be determined by multiplying the one-time Unit Price set forth in the Managed Services Price Table for the applicable Future Hardware Purchases by a lease factor. The Parties will move from the annual Capital Payments contemplated above to the monthly hardware Unit Prices through the Change Order Process and the Governance Process.

Service Provider will not be responsible for paying any Service Level Credits associated with delays caused by the Province not funding the Capital Payment in April of the Contract Year in which the Province moves from the annual Capital Payments to the monthly hardware Unit Prices.

2.7.6 Equipment not Included in the Capital Payment

For greater clarification, the following equipment is not included in the Capital Payments and is part of the monthly Unit Prices set forth in the Managed Services Price Table:

(a) Servers less than (monthly hardware Unit Price) ("**Non-Capital Servers**");

(b) Service Provider tool and lab Servers, regardless of value (SDO&G component); and

(c) network less than (SDO&G component).

2.7.7 Reduction of Non-Capital Servers

If a Client Ministry wishes to cancel a Non-Capital Server from the Managed Services after it has been procured by the Service Provider on behalf of the Client Ministry, then:

(a) the Client Ministry will provide a notice of cancellation to the Service Provider through the Province Ordering System (the "**Cancellation Notice**");

(b) the Client Ministry will pay a one-time cancellation fee to the Service Provider in an amount that is equal to:

(i) the monthly hardware Unit Price, multiplied by

(ii) the number of months that is equal to:

(A) 60 months, less

(B) the number of months the Client Ministry has been paying the monthly hardware Unit Price for the Non-Capital Server; and

(c) the Service Provider will invoice the Client Ministry for such cancellation fee in lieu of the continuing monthly hardware Unit Price for the Non-Capital Server;

(d) the Non-Capital Server will become Available Inventory under the Schedule 5A (*Server Management Services SOW*);

(e) any Available Inventory that is redeployed will be subject to a one-time Refresh Install Unit Price at the time of redeployment, as more particularly described under Section 2.3.5 (*Refresh Server Installations*) above.

2.7.8 Ownership of Hardware

All hardware, funded by the Capital Payment hardware and the non-capital payment Unit Price, is owned by Service Provider during the Term. Refer to Schedule 38 (*Termination Fees*) for ownership of the hardware following the expiry or earlier termination of the Term.

2.7.9 Disposal of hardware

Service Provider is responsible for managing the process of hardware disposal, both Capital Payment hardware and the non-capital payment hardware.

2.7.10 Treatment of Hardware for Broader Public Sector

The Parties will work together to determine the hardware treatment for the Broader Public Sector that meets the needs of both Service Provider and the Broader Public Sector entities. Such treatment may include a capital payment program similar to the Capital Payments to be made by the Province under this Schedule, or may be based upon a monthly Unit Price for the hardware. If the hardware treatment for the Broader Public Sector entities is based upon a monthly Unit Price, then the hardware prices in the Managed Services Price Table will be updated through the Change Order Process to change one-time capital Unit Prices to monthly Unit Prices, as applicable (and any such monthly Unit Prices will include any applicable leasing costs).

2.7.11 Credit Rating Adjustment to Monthly Unit Prices

If the Service Provider provides a Broader Public Sector entity with hardware based upon a monthly Unit Price, then the monthly Unit Price for that Broader Public Sector entity will be adjusted to reflect that entity's credit rating where that Broader Public Sector entity's credit rating is not as good as the Province's (unless the Province provides a guarantee to the Service Provider for the payment of the monthly Unit Price for the hardware for as long as such payments are required to made by the Broader Public Sector entity).

3. VOLUMES AND VOLUME BANDING

3.1 Summary

The purpose of this Article is to:

(a) establish baseline volumes for when volume banding, and minimum and maximum quantities apply;

(b) establish how the Unit Prices in the Managed Services Price Table change as volumes increase and decrease; and

(c) set forth the process to be followed when the minimum or maximum of the volume band ranges are achieved.

3.1.2 Volume Band Ranges

Where volume banding applies to the Unit Prices in the Managed Services Price Table (the "**Volume Banding**"), the Parties have agreed to volume bands within specified minimum and maximum volumes for each unit or service being measured (the "**Volume Band Ranges**"), as more particularly described in the Table under Section 3.2 (*Baseline Volumes & Volume Banding Table*) below (the "**Volume Banding Table**"). Where a Volume Band Range is indicated for a particular unit or service in the Volume Banding Table (such that a minimum and maximum

volume is listed), the Parties have not priced the unit or service for volumes outside of the Volume Band Range so noted, and will do so through the Change Order Process if required. Where the volumes are less than the minimum volume in the Volume Band Range, the new Unit Prices that are required as a result will take into account:

(a) diseconomies of scale to the "Service Management" component of the Unit Price; and

(b) any potential changes to SDO&G while taking into account fixed costs that Service Provider may not be able to reduce or redeploy.

3.1.3 Individual Volume Bands

The Volume Band Range for each particular unit or service being measured is broken down into individual volume bands that are expressed as ranges (each, an "**Individual Volume Band**"). Each Individual Volume Band for a particular unit or service has a different Unit Price associated to it, as described below. When the actual volumes of that unit or service cross from one Individual Volume Band to another, then all of the volume for that unit or service will be subject to the Unit Price applicable to that Individual Volume Band.

3.1.4 Individual Volume Bands and Unit Prices

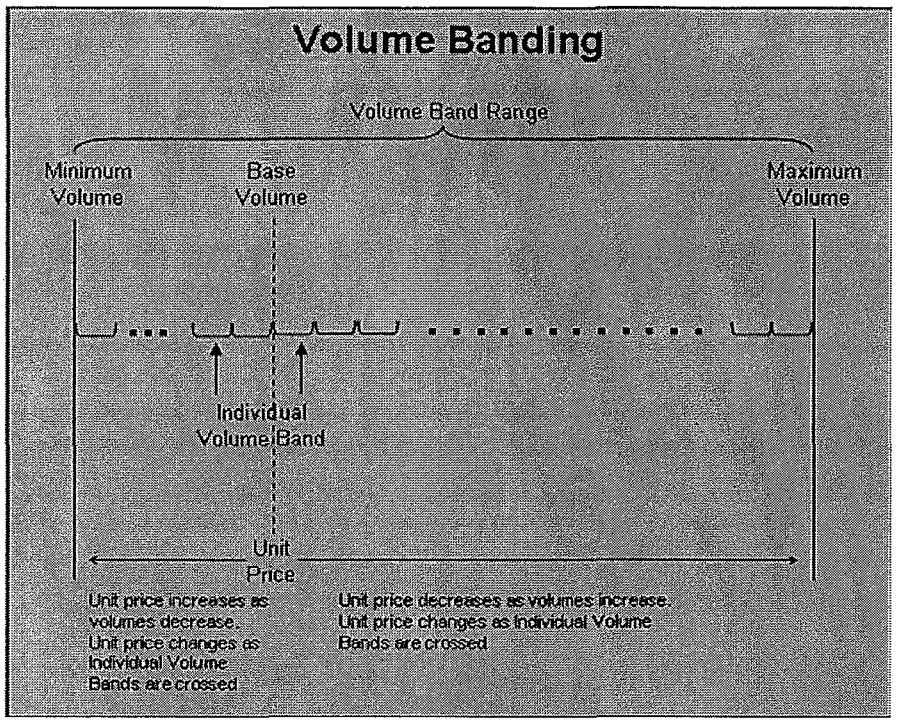
The Unit Prices applicable to any particular Individual Volume Band are expressed as an increase or decrease (each, a "**Volume Band Adjustment**") to a base price for the unit or service in question (the "**Base Unit Price**"). The Base Unit Prices are set forth in the Managed Services Price Table for each unit or service being measured, on an annual basis by Contract Year, and represent the price for the unit or service in question at the "Baseline Volume" set forth in the Volume Banding Table below. For example, the Volume Band Adjustment for a particular Individual Volume Band may be expressed as "+$1.10" or "-$0.95", which is the increase or decrease to be applied to the Base Unit Price to arrive at the Unit Price for that Individual Volume Band.

Notwithstanding any other provision of this Schedule, any reference in this Schedule to the "Unit Price in the Managed Services Price Table" means:

(a) where Volume Banding applies, the Base Unit Price, as adjusted for inflation pursuant to Section 6.3 (*Managed Services Inflation*) below, and as adjusted by the applicable Volume Band Adjustment; and

(b) where Volume Banding does not apply, the Unit Price as adjusted for inflation pursuant to Section 6.3 (*Managed Services Inflation*) below.

The Figure below provides a generic illustration of the Volume Banding.



3.2 Baseline Volumes & Volume Banding Table

The Volume Banding Table below sets forth the baseline volumes used to determine the Base Unit Prices.

Managed Services Volume Banding Category	Minimum	Individual Volume Bands (Decrements)	Baseline Volumes	Individual Volume Bands (Increments)	Maximum
Midrange					
Physical Servers and Virtual Servers	1,312		1,811 Servers		3,660
Physical Server hardware	N/A	N/A	N/A	N/A	N/A
Virtual Server hardware and hardware support	N/A	N/A	N/A	N/A	N/A
Citrix Server support	60	N/A	120 Servers	N/A	N/A
Shared File Print Services	30,001		37,000 users		46,999
Shared Databases Services	111		150 Database		300
Shared Web Services	188		247 websites		502
Dedicated Web Services (no. of instances of web hosting software)	200	N/A	300	N/A	N/A

Managed Services Volume Banding Category	Minimum	Individual Volume Bands (Decrements)	Baseline Volumes	Individual Volume Bands (Increments)	Maximum
Initial and refresh install	N/A	N/A	N/A	N/A	N/A
Optional midrange services	N/A except for extended support	N/A except for extended support	N/A except for extended support	N/A except for extended support	N/A except for extended support
Extended support hours 5X12 or 7X24	• 325 Windows Servers or • 100 Unix Servers	N/A	• 325 Windows Servers or • 100 Unix Servers	N/A	N/A
Mainframe					
Mainframe Processing (MIPs)	260 MIPs		617 MIPs		2,519
Mainframe – Non-Standard Software	NA		1	N/A	NA
Mainframe – DASD	NA	N/A	3,525 GB	N/A	NA
Mainframe – Tapes	NA	N/A	145,000 GB	N/A	NA
Optional mainframe services					
Form/print/end user support	12 Months	N/A	N/A	N/A	N/A
SAS 70 audit	N/A	N/A	N/A	N/A	N/A
Extra DR test	N/A	N/A	N/A	N/A	N/A
Database hourly support	8 hours in a 1 day period	N/A	N/A	N/A	N/A
Storage					
Managed Storage	735,721 GB		853,114 GB		1,775,719 GB
Managed Backup	786,859 GB		1,372,094 GB		2,736,857 GB
Extended Retention	2,907,951 GB		3,657,950 GB		7,157,949 GB
Optional storage services	See Optional Storage Service table below for additional details				
Archive Storage Repository	9,216 GB		50,176 GB		91,136 GB

At issue for Inquiry

3.3 Unit Prices for Different Individual Volume Bands

The Unit Price for the different Individual Volume Bands changes as a result of the following:

(a) in the case of volume increases:

(i) a higher SDO&G cost is spread over a higher volume;

(ii) the "Service Management" component of the Unit Price remains constant as volumes increase; and

(iii) the unit price adjustment (UPA) (as described below) is spread over a higher volume; and

(b) in the case for volume decreases:

(i) the same SDO&G cost is spread over a lower volume;

(ii) the same unit price adjustment (UPA) (as described below) is spread over a lower volume; and

(iii) in the case of the shared services (SFP, Shared Web and Shared Database) the same fixed costs are spread over a lower volume.

3.4 Cost of Ownership Reconciliation

The Parties acknowledge and agree that the Fees in Contract Years 1 to 3 are reduced to provide the Province with a total cost of ownership for the Managed Services that is similar to the Province's budget to perform such services internally, immediately prior to the Hand-Over Date. As a result, the Unit Prices in Contract Years 4 to 12 have been increased to partially offset the Contract Years 1 - 3 reductions described in this Section. The Parties agree to ensure the Province achieves the reductions in Contract Years 1 to 3 and the increases in Contract Years 4 to 12 as planned in the Baseline Fees (as set forth in the Baseline Fees Table in Appendix C), despite adjustments to baseline volumes in Appendix C. The Parties have attempted to set the Volume Banding of the Unit Prices associated with volume increases and decreases to accommodate this dynamic. The Baseline Fees for each Contract Year and the components that make up the Baseline Fees are presented in the Baseline Fees Table in Appendix C.

Within 30 days after the Effective Date, the Parties will create a report (the "**Reconciliation Report**"), in the form and level of detail of the Baseline Fees Table in Appendix C. The Service Provider will, on a semi-annual basis, deliver to the Province the Reconciliation Report, based on monthly tracking, that demonstrates that the expected reductions and increases included in the Baseline Fees have occurred. The Service Provider will provide a copy of the Reconciliation Report to the Province:

(a) on or before October 31st in each Contract Year, containing the information from April 1st to September 30th of that same Contract Year, and

(b) on or before April 30th containing the information from April 1st to March 31st of the previous Contract Year.

Any adjustment as a result of the April 30th Reconciliation Report will occur on the next invoice.

After the Effective Date, the Parties will work together to develop a simplified form of the Reconciliation Report, having regard to the time and effort required by the Service Provider to prepare such a Reconciliation Report in the form and level of detail as in the Baseline Fees Table in Appendix C.

3.5 Volume Band Adjustments to Unit Price

3.5.1 General

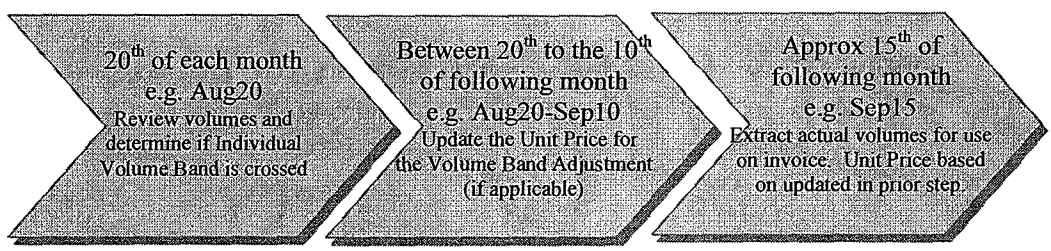
The Volume Band Adjustment to the Base Unit Price as a result of increases and decreases to volumes are applied to all the volumes of the unit or service measured within the Individual Volume Band. For greater clarification, the Volume Band Adjustment does not only apply to the incremental volume or the number of decreased units.

Once a higher Individual Volume Band is reached, the Volume Band Adjustment is applicable so long as the volumes remain at the required volume level for that band. If volumes reduce and cross into a lower Individual Volume Band, then the Volume Band Adjustment will be updated to reflect the change to the Unit Price for the revised volumes.

3.5.2 Timing of Updates for Volume Band Adjustments

The Volume Band Adjustment is set for the following month's invoice on approximately the 20th of each month. Service Provider will notify the Province if an Individual Volume Band has been crossed and that the Volume Band Adjustment will be applied to the Unit Price on the next month's invoice. The monthly invoice will be based upon the actual volumes (as per Section 7.3.5 (*Volumes for Invoicing*) and the Unit Price as set during the Volume Band Adjustment determination in the prior month.

For example, on August 20, volumes are reviewed and if an Individual Volume Band has been crossed, then a Volume Band Adjustment is made for the September 15 invoice. The September 15 invoice is based on actual volumes at that time multiplied by the Unit Price as adjusted for the Volume Band Adjustment determined on August 20. If the volume changes between August 20 and September 15, cross an Individual Volume Band, then the associated Volume Band Adjustment occurs the following month.



3.6 Midrange – Volume Band Adjustment

3.6.1 Server Management Services

The Server Management Services Unit Price will change as the total number of physical Servers and Virtual Servers, taken together, varies from the total Server baseline volume in the Volume Banding Table, and as Individual Volume Bands are crossed.

If the number of Virtual Servers increase by and the number of physical Servers decrease by then the total volume of Servers has increased by resulting in the number of Servers crossing an Individual Volume Band, then a Volume Band Adjustment applies and the Unit Price will change. At issue for Inquiry

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to all Servers, regardless of Server type, for Individual Volume Bands for the Servers based upon decrements of and increments of the baseline volume for the Servers set forth in the Volume Banding Table. Although the Individual Volume Bands for the Servers is based upon he Province may change Server volumes one Server at a time. At issue for Inquiry

The Parties expect that the 50 unit Individual Volume Bands will result in the Server Unit Prices changing twice a year. If the Province crosses over to a new Server Individual Volume Band more than twice in a Contract Year, then the Parties may discuss changing the Individual Volume Bands from to a higher number of units through the Change Order Process. At issue for Inquiry

The following are examples of how the Server Volume Band Adjustment applies to volume increases and volume decreases.

Example 1:		
Total Server count above total baseline Server volume in December 2013		
Midrange physical and Virtual Server volume at December 2013 billing date	1,911 Servers	A
Baseline total Server volume - physical and Virtual Servers	1,811 Servers	B
Variance to baseline total Server volume [A - B]	+ 100 Servers	
Application of midrange Volume Band Adjustment to specific Server type:		
December 2013 monthly Unit Price : Server Management Services -Tier 2 for small Windows Application, Database, or Web Server		
2013/14 per unit decrease to monthly Unit Price for Individual Volume Band applicable to Server increase (Appendix D)	At issue for Inquiry	
December 2013 monthly Unit Price: Server Management Services -Tier 2 for small Windows Application, Database, or Web Server		

Example 2:		
Total Server count below total baseline Server volume in December 2013		
Midrange physical and Virtual Server volume at December 2013 billing date	1,462 Servers	A
Baseline total Server volume - physical and Virtual Servers	1,812 Servers	B
Variance to baseline total Server volume [A - B]	(350) Servers	
Application of midrange Volume Band Adjustment to specific Server type:		
December 2013 monthly Unit Price: Service Management -Tier 2 for small Windows Application, Database, or Web Server		
2013/14 per unit increase to monthly Unit Price for Individual Volume Band applicable to Server decrease (Appendix D)	At issue for Inquiry	
December 2013 monthly Unit Price: Service Management -Tier 2 for small Windows Application, Database, or Web Server		

3.6.2 Server Hardware

There is no Volume Band Adjustment required for Server hardware (including for physical Host Servers used to host Virtual Servers):

(a) as volume increases use the same hardware Unit Price as in the Managed Services Price Table associated with the applicable Contract Year whether the hardware is greater than and part of the Capital Payment or less than and part of a monthly hardware Unit Price.

At issue for Inquiry

(b) as volume decreases are addressed through:

(i) a Cancellation Fee for Servers (excluding physical Host Servers) where the monthly Unit Price applies (refer to Section 2.7.7 (*Reduction of Non-Capital Servers*);

(ii) the hardware was part of the Capital Payment and the Province has fully funded the purchase of the hardware; or

(iii) the Service Provider is responsible for decreases to the physical Host Servers that are not included in a Capital Payment.

3.6.3 Physical and Virtual Server Installation

There is no Volume Band Adjustment required for Server installations as volume increases use the same Unit Price as in the Managed Services Price Table associated with the applicable Contract Year.

There is no Volume Band Adjustment required for Server installations as volume decrease, since the Server installation Unit Price is paid for by the Province in the month the installation occurs (the cost of installation is not spread over a period of time).

3.6.4 Shared File and Print Services

The Share File and Print Services (SFP) Unit Price will change as the actual user volume varies from the baseline user volume set forth on the Volume Banding Table, and as Individual Volume Bands are crossed. Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the number of SFP users based upon and the baseline volume for the SFP users. Although the Individual Volume Bands for the SFP users is based upon the Province may change SFP user volumes one user at a time.

At issue for Inquiry

Example 4:		
Total SFP user count below total baseline SFP volume in January 2012		
Total SFP Services user volume at January 2012 billing date	34,655 users	A
Baseline SFP Services user volume	37,000 users	B
Variance to baseline total SFP Services user volume [A - B]	(2,345 users)	
Application of Volume Band Adjustment to SFP Services :		
January 2012 baseline monthly Unit Price : SFP Services		
2012/13 per unit increase to baseline monthly Unit Price for Individual Volume Band applicable to SFP Services user decrease (Appendix D)		
January 2012 adjusted baseline monthly Unit Price SFP Services user		

At issue for Inquiry

3.6.5 Shared Web Services

The Shared Web Service Unit Price will change as the actual number of websites varies from the baseline website volume set forth in the Volume Banding Table, and as Individual Volume Bands are crossed.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the number of websites based upon the baseline volume for the number of websites. Although the Individual Volume Bands for the number of websites is based upon the Province may change website volumes one website at a time.

At issue for Inquiry

Refer to the SFP example above for how to apply Volume Banding to Shared Web.

3.6.6 Shared Database Services

The Shared Database Service Unit Price will change as the actual number of Databases varies from the baseline Database volume set forth in the Volume Banding Table, and as Individual Volume Bands are crossed.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the number of Databases based upon the baseline volume for the number of Databases. Although the Individual Volume Bands for the number of Databases is based upon the Province may change Database volumes two Databases at a time (because there must be a production and a development/test Database in each instance).

At issue for Inquiry

Refer to the SFP example for how to apply Volume Banding to Shared Database.

3.6.7 Other Midrange Services and Optional Midrange Services

For other Server Management Services and Optional Midrange Services not mentioned in this Article, there are no Volume Band Adjustments required as volumes increase or decrease. The same Unit Price as in the Managed Services Price Table for the applicable Contract Year will apply to all volumes for the other Server Management Services and Optional Midrange Services.

The 5X12 and 7X24 Extended Support Hours both require minimum volumes in order for the Extended Support Hours service to be available for the Server Management Services. The minimum volumes apply on a per Server category, as indicated in the Volume Banding Table above.

3.7 Mainframe Processing Services

3.7.1 Mainframe Processing Service Support

The Mainframe Processing Services Unit Price will change as the installed number of MIPS varies from the baseline MIPS volume set forth in the Volume Banding Table, and as Individual Volume Bands are crossed.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the Mainframe Processing Services based upon the baseline volume of 617 MIPS. Although the Individual Volume Bands for the Mainframe Processing Services is based upon the Province may change the MIPS volumes by If the Province crosses an Individual Volume Band for the Mainframe Processing Services more than once in any 12 month period, then Service Provider will be entitled to include an additional change fee in respect thereof as part of the Change Order Process. At issue for Inquiry

For greater clarification the Unit Price in the Managed Services Price Table for the Mainframe Processing Services applies equally to the IBM Z9 and Z10 processing hardware.

Example 5: **Total MIPS volume above total baseline MIPS volume in September 2014**		
Total MIPS volume at September 2014 billing date	687 MIPs	A
Baseline total MIPS volume	617 MIPs	B
Variance to baseline total MIPS volume [A - B]	+ 70 MIPs	
Application of Mainframe Processing Volume Band Adjustment:		
September 2014 monthly Unit Price : Mainframe Processing		
2014/15 per unit decrease to monthly Unit Price for Individual Volume Band applicable to increase (Appendix D)	At issue for Inquiry	
September 2014 monthly Unit Price: Mainframe Processing		

Example 6: **Total MIPS volume below total baseline MIPS volume in September 2014**		
Total MIPS volume at September 2014 billing date	497 MIPs	A
Baseline total MIPS Volume	617 MIPs	B
Variance to baseline total MIPS volume [A - B]	(120) MIPs	
Application of Mainframe Processing Volume Band Adjustment:		
September 2014 monthly Unit Price: Mainframe Processing		
2014/15 per unit increase to monthly Unit Price for Individual Volume Band applicable to decrease (Appendix D)		
September 2014 monthly Unit Price: Mainframe Processing		

At issue for Inquiry

3.7.2 Mainframe DASD and Tape Services

Mainframe DASD Services and Tape Services do not require Volume Band Adjustments as volumes increase or decrease. The same Unit Price as in the Managed Services Price Table for the applicable Contract Year will apply to all volumes of the Mainframe DASD Services and Tape Services.

There may be additional hardware requirements for DASD and Tape volume increases, as more particularly described in Section 2.4.6 (*Mainframe Hardware*) above.

3.8 Managed Storage and Managed Backup Services

3.8.1 Managed Storage

The Managed Storage Unit Price (Tier 1, 2, 3 and NAS) will change as the total number of allocated storage GBs, taken together, varies from the total storage GB baseline volume in the Volume Banding Table, and as Individual Volume Bands are crossed. For greater clarification, the storage GB volume excludes the storage volumes in support of the "Midrange Shared Services" which is addressed separately in Section 2.3 (*Midrange Shared Services*) above.

If the total Managed Storage volume for Tier 1 increases by GBs and the Tier 3 decreases by GBs, then the total volume of storage GBs has increased by GBS crossing an Individual Volume Band. A Volume Band Adjustment will therefore apply and the Unit Price will change.

Notwithstanding the aggregating of the Tier 1, 2 and 3 storage for purposes of determining Individual Volume Bands, it there is a material decrease in any one Tier of storage (in the aggregate), then a cancellation fee for that Tier of storage may apply through the Change Order Process to address any annually prepaid maintenance for that Tier of storage.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the storage GBs, regardless of storage type (Tier 1, 2, 3 and NAS), for the Individual Volume Bands based upon decrements of GBs below, and increments of GBs above, the baseline GB volume set forth in the Volume Banding Table. Although the Individual Volume Bands for the storage GBs is based upon increments and decrements of the Province may change the Tier 1, 2 and 3 storage by volumes at a time through each Province

Ordering System request, and the NAS storage by volumes of At issue for Inquiry GBs at a time through each Province Ordering System request.

Example 7: **Total Managed Storage volume above total baseline Managed Storage volume in November 2011**		
Total Managed Storage volume at November 2011 billing date	939,720 gigs	A
Baseline total Managed Storage volume - Tier 1/2/3/NAS	855,720 gigs	B
Variance to baseline total Managed Storage volume [A - B]	+ 84,000 gigs	
Application of Managed Storage Volume Band A adjustment to specific storage type:		
November 2011 monthly Unit Price: Tier 2 Managed Storage - Service Provider Owned		
2011/12 per unit decrease to monthly Unit Price Individual Volume Band applicable to Managed Storage increase (Appendix D)	At issue for Inquiry	
November 2011 monthly Unit Price: Tier 2 Managed Storage - Service Provider Owned		

Example 8: **Total Managed Storage volume below total baseline Managed Storage volume in November 2011**		
Total Managed Storage volume at November 2011 billing date	760,720 gigs	A
Baseline total Managed Storage volume - Tier 1/2/3/NAS	855,720 gigs	B
Variance to baseline total Managed Storage volume [A - B]	(95,000) gigs	
Application of Managed Storage Volume Band Adjustment to specific storage type:		
November 2011 monthly Unit Price: Tier 2 Managed Storage - Service Provider Owned		
2011/12 per unit increase to monthly Unit Price for Individual Volume Band applicable to GB Managed Storage decrease (Appendix D)	At issue for Inquiry	
November 2011 monthly Unit Price: Tier 2 Managed Storage - Service Provider Owned		

3.8.2 Managed Backup and Restore Services

The Managed Backup and Restore Services Service Unit Price will change as the actual number of backup GBs varies from the baseline backup GB volume set forth in the Volume Banding Table, and as Individual Volume Bands are crossed. For greater clarification, the backup GB volume excludes the backup volumes in support of the "Midrange Shared Services" which is addressed separately in Section 2.3 (*Midrange Shared Services*) above.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the backup GBs for the Individual Volume Bands based upon decrements of GBs below, and increments of GBs above, the baseline backup GB volume set forth in the Volume Banding Table. Although the Individual Volume Bands for the backup GBs is based upon increments and decrements of GBs, the Province may change the backup volumes GB at a time.

At issue for Inquiry

Refer to the Managed Storage example for how to apply Volume Banding to backup.

3.8.3 Extended Retention

The Extended Retention Services Unit Price will change as the actual number of retention GBs varies from the baseline retention GB volume set forth in the Volume Banding Table, and as Individual Volume Bands are crossed. For greater clarification, the retention GB volume excludes the retention volumes in support of the "Midrange Shared Services" which is addressed separately in Section 2.3 (*Midrange Shared Services*) above.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the retention GBs for the Individual Volume Bands based upon decrements of GBs below, and increments of GBs above, the baseline backup GB volume set forth in the Volume Banding Table. Although the Individual Volume Bands for the retention GBs is based upon increments and decrements of GBs, the Province may change the retention volumes GB at a time. At issue for Inquiry

Refer to the Managed Storage example for how to apply Volume Banding to Extended Retention.

3.9 Hardware, Software and Installation (Storage, Backup and Retention)

The Province will fund all storage, backup and retention hardware, software and installations (including for the Optional Storage Services described below) through the Capital Payments. There may be additional hardware, software and installations required for volume increases, which will be funded through the Capital Payment.

3.10 Optional Storage Services

3.10.1 File System Archive Storage Services

Archive Storage Repository

The Archive Storage Repository Unit Price will change as the actual number of storage GBs varies from the baseline storage GB volume set forth in the Volume Banding Table, and as Individual Volume Bands are crossed.

Appendix D (*Volume Band Adjustments*) includes the Volume Band Adjustments applicable to the archive storage GBs for the Individual Volume Bands based upon decrements of GBs below, and increments of GBs above, the baseline archive storage GB volume set forth in the Volume Banding Table. Although the Individual Volume Bands for the archive storage GBs is based upon increments and decrements of GBs, the Province may change the archive storage volumes GBs at a time. At issue for Inquiry

Refer to the Managed Storage example for how to apply Volume Banding to Archive Storage Repository.

File Archive Storage (FAS)

The File Archive Storage Repository can be purchased in addition to the Archive Storage Repository, and must be purchased in corresponding volumes to the Archive Storage Repository (as the Archive Storage Repository increases or decreases). The File Archive Storage Repository monthly Unit Price is set forth in the Managed Services Price Table, and is not subject to Volume Banding. The File Archive Storage must be subscribed for a 12 month period, and any early termination of such 12 month service may be subject to cancellation fees for fixed annual costs (such as for the cost of Server access fees).

3.10.2 Other Optional Storage Services

Optional Storage Services	**Comments/Notes**
Tier 1, Mirrored Primary	No minimum volume required to obtain service
Tier 2, Mirrored Primary	No minimum volume required to obtain service
Tier 1, with Local Clone Services, Mirrored Primary	See Note 1 and 3 below
Tier 1, with Local Clone Services, at Same Site - Standard	See Note 1 and 3 below
Tier 1, with Replication Services and Local Clone Services, Mirrored Primary	See Notes 1, 2 and 3 below
Tier 1, with Replication Services and Local Clone Services, Standard	See Notes 1, 2 and 3 below
Tier 1, with Replication Services, Standard	See Note 2 and 3 below
Tier 1, with Replications Services, Mirrored Primary	See Note 2 and 3 below
Archive Storage Repository	See Section 3.10.1 (*File System Archive Storage Services*) above
Files System Archive (FSA)	See Section 3.10.1 (*File System Archive Storage Services*) above
VTL Backup to Encrypted Offsite Tape Service	Any volumes will count as backup volumes as described in Section 3.8.2 (*Managed Backup and Restore Services*) above

Note 1: The other Optional Storage Services that include Local Clone Services must be acquired in multiples of All Optional Storage Services that include Local Clone Services aggregate towards increments.

Note 2: The other Optional Storage Services that include Replication Services must be acquired in multiples of All Optional Storage Services that include Replication Services aggregate towards the increments.

At issue for Inquiry

Note 3: The other Optional Storage Services must be subscribed for as a 12 month service, and any early termination of such 12 month service may be subject to cancellation fees for fixed annual costs (such as for the cost of annual maintenance fees).

3.11 STMS Data Centre Services

The VA Price Table (defined below) contains the changes to the VA Unit Price as a result of changes in the VA volumes at the STMS Data Centres, applicable to both the Province and the Broader Public Sector. Section 4 (*Data centre unit prices (VAs)*) describes how the VA Unit Price changes as VA volumes increase and decrease.

3.12 Costs not Addressed Through Volume Banding – Network

The Volume Band Adjustments to the Unit Prices do not include special network requirements for the Province (for example, as of the Hand-Over Date, S15 S15 Changes to the network architecture (for example, if a Ministry other than S15 wishes to be in a separate compartment, or has other special network requirements) will be handled through the Change Order Process.

The network infrastructure has a finite capacity and when the capacity is reached, additional infrastructure and support is required. When Province network capacity requirements increase, beyond the network infrastructure capacity, a Change Order is required.

3.13 Unit Prices and the Broader Public Sector

The Unit Prices and Volume Band Adjustments will apply to BPS Services Agreements. Each Broader Public Sector entity may contract for all of the Services or some combinations of Services (such as storage or Servers), but the Broader Public Sector entity may not:

(a) separate the storage, backup and retention services;

(b) select Optional Midrange Services or Citrix Server Support without contracting for Server support under the Server Management Services. The shared services (Shared File Print, Shared Database and Shared Web) are available separately from the Server support under the Server Management Services; and

(c) select hardware without the associated support services.

The Unit Prices and Volume Band Adjustments do not include the following costs which will be determined at the time the Broader Public Sector entity enters into a BPS Services Agreement:

(d) Transformation – migration of the Broader Public Sector entity's existing equipment, applications and data to the STMS Data Centres; integration and transformation of the Broader Public Sector entity's current environment to the Managed Services described in the SOWs; and incremental operating costs required to support the existing Broader Public Sector infrastructure until the Transformation is complete ;

(e) changes to the Services described in the SOWS, or special requirements (both technical solution and business requirements),that impact the Unit Prices. For example, a unique request by the Broader Public Sector entity that requires changes to how the Services are delivered such as security, reporting, invoicing, service management, or higher CRM effort;

(f) Network – Unless provided by the Broader Public Sector entity, the following network components will be required to connect the Broader Public Sector entity to the Managed Services:

(i) circuits from the Broader Public Sector location into the STMS Data Centres;

(ii) circuits between the STMS Data Centres;

(iii) incremental network hardware within the STMS Data Centres; or

(iv) changes to existing network hardware in the STMS Data Centres; and

(g) if the Broader Public Sector entity chooses to provide its own network components, then the Broader Public Sector entity will pay for the Service Provider to support the network.

In the case where the BPS Services Agreement is for one of the Storage Services or Server Management Services, there will be additional transformation and operating costs associated with connecting the two Managed Services.

The Parties will determine the appropriate manner for adjusting the Unit Prices in the Managed Services Price Table to account for the fees described above. These fees may be dealt with as one-time fees or may be added as a new component to the Unit Prices in the Managed Services Price Table, as determined by the Parties.

The Unit Price for a Broader Public Sector entity will not include the "unit price adjustment component" of the Unit Prices in the Managed Services Price Table as this component is unique to the Province.

4. DATA CENTRE UNIT PRICES (VAS)

4.1 Summary VA Fees

The "**VA Unit Price**" is the monthly unit pricing within each of the STMS Data Centres as set forth in Appendix A – *VA Price Tables* (the "**VA Price Tables**"), and is based upon the Volt Amps ("**VA**") unit pricing for the Province VA Commitment (defined below) for each of the STMS Data Centres. The VA Unit Price includes payment for such things as space, power and cooling, fire systems, security, onsite amenities and certain support, all as more particularly described in Schedule 2 (*Data Centre Services SOW*) (the "**Data Centre SOW**"). The VA Unit Price for each STMS Data Centre multiplied by the Province VA Commitment for each STMS Data Centre will determine the monthly "**VA Fees**" payable by the Province to the Service Provider.

For greater clarification, the Province VA Commitment will be available within two data centres that comprise the STMS Data Centres: (a) the STMS Interior Data Centre, which is a new data centre construction project that will start after the Effective Date; and (b) the STMS Calgary Data Centre, which is a new data centre construction project already under construction.

4.2 Summary of Province VA Commitment

The Province Initial VA Commitment (defined in Section 4.4 (*Availability Dates and Province Initial VA Commitment*) below) in each STMS Data Centre at the Effective Date may be increased on or before June 30, 2009 to the Province Revised Initial VA Commitment (defined in Section 4.6 (*Increases to the Province Initial VA Commitment by June 30, 2009*) below). The Province Initial VA Commitment or Province Revised Initial VA Commitment, as applicable, may be increased from time to time (the "**Province Additional VA Commitment**") in accordance with Section 4.9 (*Increases to the Province VA Commitment*) below, and the resulting increased commitment may be decreased from time to time in accordance with Section 4.10 (*Reduction to Province Additional VA Commitment*)below (the resulting aggregate VA commitment, taking into account all such permitted increases and decreases is referred to as the "**Province Adjusted VA Commitment**").

For purposes of this Schedule, all references to the "**Province VA Commitment**" means the Province Initial VA Commitment, the Province Revised Initial VA Commitment, or the Province Adjusted VA Commitment, as applicable, for each STMS Data Centre. For greater clarity, each STMS Data Centre has its own Province VA Commitment.

4.3 Summary of VA Price Tables

There are three STMS Data Centre VA Price Tables in Appendix A - *VA Price Tables*:

(a) Table A: STMS Calgary Data Centre – VA Price Table;

(b) Table B: STMS Interior Data Centre – VA Price Table (where expansion of the data centre results from a request of the Province); and

(c) Table C: STMS Interior Data Centre – VA Price Table (where expansion of the data centre results from Service Provider initiative).

Table B STMS Interior Data Centre in the VA Price Tables contains a number of cells that are shaded 'grey' with no VA Unit Price. These 'grey' shaded cells indicate onsite expansion limitations of the overall size of the STMS Interior Data Centre. The prices in Table B are based on:

(i) securing a site suitable to support a data centre of at least 3,600,000 VAs in size to be built in two 1,800,000 VAs phases;

(ii) having the first 1,800,000 VA phase fully reserved before the second 1,800,000 VA phase is built; and

(iii) having at least 600,000 VA of Province VA Commitment in the second phase prior to it being built.

As a result of paragraphs (i) to (iii) above, the 'grey' cells in Table B indicate the second phase which may not be available to meet a Province request for Province VA Commitment unless there is sufficient demand for the Service Provider to initiate the second phase. If the Service Provider initiates the second phase build of STMS Interior Data Centre, then the pricing shown in the 'grey' cells in Table C STMS Interior Data Centre.

In both Table B and C the STMS Interior Data Centre site is based on a maximum of 3,600,000 VA in size and as such any cells in Tables B and C that correspond to 3,600,000 VA or greater do not contain a VA Unit Price and are shaded 'black'.

4.4 Availability Dates and Province Initial VA Commitment

The monthly VA Fees for the Province Initial VA Commitment or Province Revised Initial VA Commitment, as applicable, at each STMS Data Centre will commence once:

(a) the Availability Date for such Province VA Commitment occurs; and

(b) the WTS Customer Environment is ready and available for use by the Province.

For greater clarity, when the WTS Customer Environment is ready, the monthly VA Fees for the Province Initial VA Commitment or Province Revised Initial VA Commitment, as applicable will commence. Where the monthly VA Fees invoiced to the Province have been reduced by the number of VAs allocated to a Broader Public Sector entity under a BPS Services Agreement.

The Service Provider may (at its sole discretion) provide an earlier Availability Date than set forth in the table below (the "**Early Availability Date**") for some or all of the Province Initial VA Commitment or Province Revised Initial VA Commitment for a particular STMS Data Centre, which may be subject to a stated minimum number of VAs (the "**Early Capacity**"), and the Province may elect (at its sole discretion) to take advantage of such Early Availability Date through the Change Order Process, in which case: (i) the Service Provider will make the Early

Capacity for the applicable STMS Data Centre available to the Province; and (ii) the monthly VA Fees for the Early Capacity will commence on the Early Availability Date.

The "**Province Initial VA Commitment**" is the amount of VA capacity that has been reserved by the Province in a given STMS Data Centre at the Effective Date.

The following table shows the Province Initial VA Commitment at the Effective Date for each of the STMS Data Centres and the respective expected Availability Dates for the Province.

STMS Data Centres	Province Initial VA Commitment	Expected Availability Date
STMS Interior Data Centre	1,200,000 VAs	24 months after Effective Date
STMS Calgary Data Centre	300,000 VAs	November 1, 2009

4.5 Allocation and Reallocation of the Province VA Commitment

Within the Province VA Commitment, the Province will allocate (or reallocate) VAs to Broader Public Sector entities who enter into BPS Services Agreements with the Service Provider (each, a "**BPS Customer**"). Any such allocation (or reallocation) of VAs out of the Province VA Commitment are not additive but are part of the Province VA Commitment. Throughout the Term the Province:

(a) will manage and be responsible for the total Province VA Commitment; and

(b) through an allocation (or reallocation) process, may allocate (or reallocate) some of that VA capacity to BPS Customers through the Change Order Process (and subject to there being a corresponding Change Order from the BPS Customers to accept such allocation, as more particularly described in the BPS Services Agreements).

The process for reallocating VAs is described in the Data Centre SOW. A reallocation that requires changes to the Customer Environment may result in one-time charges, as described in Section 4.13.4 (*Customer Environment Fees – BPS Customers*) to implement the changes.

4.6 Increases to the Province Initial VA Commitment by June 30, 2009

The VA Price Tables set forth the VA Unit Prices based on the different possible Province VA Commitments where each price column (the "**VA Price Column**") is specific to a given Province Initial VA Commitment or Province Revised Initial VA Commitment (as applicable). After the Effective Date (but on or before June 30, 2009), the Province may increase the Province Initial VA Commitment at either or both of the STMS Data Centres. An increase to the Province Initial VA Commitment must be for a minimum of 5,000 VAs, where the minimum may be increased by increments of 100 VAs. Once the Province has finalized the quantity of VAs, any increase will be added to the Province Initial VA Commitment, the "**Province Revised Initial VA Commitment**". Based on the Province Revised Initial VA Commitment, the particular VA Price Column associated with the Province Revised Initial VA Commitment will be used to determine the VA Unit Price applicable to the Province for the Term. For example, if

the Province Revised Initial VA Commitment is 1,300,000 VAs in the STMS Interior Data Centre, then the VA Price Column in the VA Price Tables will be the column with the volume range of 1,200,000 to 1,499,999 with a starting VA Unit Price of

Different VA volume bands and prices are indicated in the rows of the VA Price Column (each, a "**VA Price Row**"). For greater clarification, some VA Price Rows do not have a "price" indicated for the VA volume band in question, and those "prices" will be determined in the manners more particularly described in Section 4.3 (*Summary of VA Price Tables*).

After the Province Revised Initial VA Commitment is set, if the Province crosses into the next VA Price Row as a result of Province Additional VA Commitment, then the VA Unit Price is adjusted as per the VA Price Table. For example (continuing with the example from above):

- if the Province Additional VA Commitment is 350,000 VAs (with a resulting Province Adjusted VA Commitment of 1,650,000 VAs), then the VA Price Row for this Province Additional VA Commitment will be the row with the volume range of 300,000 to 599,999;
- the VA Unit Price in the VA Price Row with the volume range of 300,000 to 599,999 is and
- the VA Unit Price for all of the Province Adjusted VA Commitment of 1,650,000 VAs will change fron

4.7 Phase-in of Province VA Commitment

"**Data Centre Month**" refers to the number of full calendar months after the Availability Date for each of the STMS Data Centres. For greater clarification, the first Data Centre Month will be on a different date for each of the STMS Data Centres as a result of the different Availability Dates for each of them.

The Province Initial VA Commitment or Province Revised Initial VA Commitment at each STMS Data Centre will be phased in over a five (5) year period commencing on the Availability Date of the STMS Data Centre according to the following schedule (the "**Capacity Phase-in**"):

(a) Data Centre Month 1 to 12 = 60% of Province VA Commitment;

(b) for the STMS Calgary Data Centre, if the Province VA Commitment for Year 1 exceeds 600,000 VAs, then the Service Provider may require at least 18 months notice for delivery of capacity in excess of 600,000 VAs. It is anticipated that the Parties will determine a suitable solution once the Province Initial VA Commitment or Province Revised Initial VA Commitment has been determined;

(c) Data Centre Month 13 to 24 = 70% of Province VA Commitment;

(d) Data Centre Month 25 to 36 = 80% of Province VA Commitment;

(e) Data Centre Month 37 to 48 = 90% of Province VA Commitment; and

(f) Data Centre Month 49 to end of Term = 100% of Province VA Commitment.

If the Province agrees to commence the Early Capacity upon the Early Availability Date, then the Early Capacity will form part of the capacity that is phased-in according to the percentage phase-in of the Province VA Commitment described above (for example, if the Early Capacity is 40% of the total Province VA Commitment for the STMS Interior Data Centre, then this 40% will form part of, and is not in addition to, the 60% Province VA Commitment for Data Centre Months 1 to 12).

4.8 Accelerated Phase-in of Capacity

The Province may request, through the Change Order Process, an acceleration to the Capacity Phase-in schedule described above for the STMS Data Centres, in which case:

(a) if there is additional VA capacity available at the applicable STMS Data Centre to accommodate the acceleration, then the additional VAs associated with the acceleration of the Capacity Phase-in will be made available to the Province within 90 days; or

(b) if the additional VA capacity is not available at the applicable STMS Data Centre to accommodate the acceleration, then the additional VAs associated with the acceleration of the Capacity Phase-in will be made available to the Province at a date agreed to between the Service Provider and the Province in the Change Order Process. Such an acceleration of the phase-in schedule will not change the Province VA Commitment for that STMS Data Centre, nor will it change the VA Unit Price.

Each request for an acceleration to the Capacity Phase-in must be for a minimum of 5,000 VAs up to a maximum of the total Province VA Commitment, where the minimum may be increased by increments of 100 VAs. By way of illustration, in Data Centre Months 1 to 12 the Capacity Phase-in at the STMS Interior Data Centre is 720,000 VAs. Accordingly, for Data Centre Months 1 to 12, the accelerated phase-in must be for at least 725,000 VAs of total capacity, increased by increments of 100 VAs (725,100 VAs, 725,200 VAs and so on) up to a maximum 1,200,000 VAs of total capacity, subject to availability.

Once an accelerated phase-in of capacity is requested, the Province cannot revert back to the original Capacity Phase-in until the original Capacity Phase-in catches up with the accelerated capacity phase-in. Once the original Capacity Phase-in has caught up with the accelerated capacity phase-in, the Province may revert back to the original Capacity Phase-in schedule. For example, if in Data Centre Months 13 to 24 the Province requests an accelerated phase-in to 90% (instead of the original Capacity Phase-in of 70%), then the Province cannot request a reduction back to the original Capacity Phase-in of 70% or any other percent less than 90%. The Province is not required to then accelerate the capacity phase-in beyond 90% until Data Centre Month 49, as per the original Capacity Phase-in schedule.

4.9 Increases to the Province VA Commitment

The following sections describe:

(a) increases to the Province VA Commitment after June 30, 2009 and up to and including Data Centre Month 60; and,

(b) increases to the Province VA Commitment during or after Data Centre Month 61.

4.9.1 Increases after June 30, 2009 and up to and including Data Centre Month 60

A Province Additional VA Commitment requested after June 30, 2009 and with an Installation Date up to and including Data Centre Month 60, is at the VA Unit Prices. A Province Additional VA Commitment must be for a minimum of 5,000 VAs, where the minimum may be increased by increments of 100 VAs. The date on which the Province Additional VA Commitment is available to the Province and the VA charges for such capacity will commence, (the "**Installation Date**").

If the applicable STMS Data Centre has the available capacity for the Province Additional VA Commitment, then the Service Provider will deliver the Province Additional VA Commitment within 90 days following receipt of a Change Order therefor from the Province. This Change Order must be received by the Service Provider by Data Centre Month 57 for a particular STMS Data Centre in order for the Installation Date to be on or before Data Centre Month 60.

If the applicable STMS Data Centre does not have the available capacity for the Province Additional VA Commitment, and if financing on commercially reasonable terms is available to the Service Provider, then the Service Provider will deliver the Province Additional VA Commitment within 18 months after receipt of the Change Order therefor from the Province. This Change Order must be received by the Service Provider by Data Centre Month 42 for a particular STMS Data Centre in order for the Installation Date to be on or before Data Centre Month 60.

If financing on commercially reasonable terms is not available to the Service Provider, as contemplated above, then the Service Provider shall provide reasonable evidence thereof to the Province.

If at the Installation Date of the Province Additional VA Commitment there is not at least 11 years remaining in the Term, then:

(a) a contract extension is required for the STMS Data Centre Services so that there is at least 11 years remaining in the Term as it relates to the Province Adjusted VA Commitment; or

(b) a VA Unit Price with an increase added to it will be applicable to the Province Additional VA Commitment, where the increase takes into account the remaining Term (being less than 11 years). The Province VA Commitment for the VAs in place before Data Centre Month 60 will continue to be charged the VA Unit Price

and the Province Additional VA Commitment will be charged the VA Unit Price with the increase added.

For example, if the Installation Date of the Province Additional VA Commitment is before contract month 48, then there is 11 years remaining in the Term and no extension is required. If the Installation Date of the Province Additional VA Commitment is during or after month 49, then there is less than 11 years remaining in the Term and the Province must select one of paragraph (a) or (b) above.

Where the Province Additional VA Commitment causes the next VA Price Row to be engaged, then the VA Unit Price applicable to the Province Adjusted VA Commitment is as per the applicable VA Price Row, and in the case where the Province selects paragraph (b), the Province Additional VA Commitment will be charged the VA Unit Price with an increase added.

For example:

- Based on Province Initial VA Commitment of 300,000 VA in the STMS Calgary Data Centre;
- and the Province Adjusted VA Commitment is 600,000 VA (therefore a Province Additional VA Commitment of 300,000 VA);
- then the VA Unit Price for all 600,000 VAs of Province Adjusted VA Commitment goes from the VA Unit Price of and the Province Additional VA Commitment of 300,000 VAs will be charged the with an increase added.

At issue for Inquiry

4.9.2 Increases during or after Data Centre Month 61

Where the Installation Date for a Province Additional VA Commitment occurs during or after Data Centre Month 61, the VA Unit Prices for the Province Additional VA Commitment in the VA Price Tables are indicative and directional only. The Service Provider shall establish, to the reasonable satisfaction of the Province, the reasons why such VA Price Tables should not apply for any such Province Additional VA Commitment after Data Centre Month 60, with regard to market conditions affecting financing, facility construction, operational costs and the remaining Term. The Parties will work together to determine an acceptable VA Unit Price which will be applied to all the VAs in the applicable Change Order.

If capacity is available at the associated STMS Data Centre to meet the request for the Province Additional VA Commitment, then the Service Provider will deliver the Province Additional VA Commitment within 90 days after the Change Order. If the VA capacity is not available to accommodate the Province Additional VA Commitment and financing on commercially reasonable terms is available, then the VAs will be available within 18 months after the Change Order.

4.9.3 Phase-in of Province Additional VA Commitments

For Change Orders of less than 300,000 VAs of Province Additional VA Commitment within a STMS Data Centre, there will be no phase-in of the Province Additional VA Commitment. For

greater clarification, the Province will be invoiced for the monthly VA Fees for the Province Additional VA Commitment starting on the Installation Date therefor and continuing until the expiry or earlier termination of the Term.

For Province Additional VA Commitment of 300,000 VAs or more within a STMS Data Centre, the Province Additional VA Commitment will either (at the option of the Province):

(a) commence at 100% of the Province Additional VA Commitment on the Installation Date; or

(b) be phased-in at 50% of the Province Additional VA Commitment for months 1 through 6 following the Installation Date, and increased to 100% of the Province Additional VA Commitment at month 7 following the Installation Date.

The option selected by the Province will be described in the Change Order for such Province Additional VA Commitment.

4.10 Reduction to Province Additional VA Commitment

Once per Contract Year, with at least 90 days prior written notice and delivered to the Service Provider in accordance with the notice provisions of Section 33.1 (*Notice*) of the Agreement, the Province Additional VA Commitment may be reduced in a given STMS Data Centre subject to the following conditions:

(a) the reduction can only be applied to the Province Additional VA Commitment for a given STMS Data Centre and cannot reduce the Province VA Commitment to below either the Province Initial VA Commitment or the Province Revised Initial VA Commitment, as applicable, for that STMS Data Centre. The reduction cannot be made to any of the Province VA Commitment that is allocated to New Data Centre Space (and accordingly, there must be sufficient VAs in the Province Additional VA Commitment that is not allocated to New Data Centre Space to account for the requested reduction);

(b) the reduction for the STMS Interior Data Centre in any one Contract Year cannot reduce the Province VA Commitment for the STMS Interior Data Centre below the greater of:

(i) the maximum Province VA Commitment previously achieved at the STMS Interior Data Centre up to the time of reduction, less 300,000 VAs; or

(ii) the Province Initial VA Commitment or the Province Revised Initial VA Commitment (as applicable) for the STMS Interior Data Centre.

For example in the STMS Interior Data Centre:

- the Province VA Commitment is 1,200,000 VAs;

- in Contract Year 8 the Province Additional VA Commitment is 400,000 VAs for a Province Adjusted VA Commitment of 1,600,000 VAs;
- in Contract Year 9 the Province reduces the Province Adjusted VA Commitment by 300,000 VAs, reducing the Province Adjusted VA Commitment to 1,300,000 VAs;
- in Contract Year 10 the Province Additional VA Commitment is 200,000 VAs for a Province Adjusted VA Commitment of 1,500,000 VAs;
- in Contract Year 11 the Province can only reduce the Province Adjusted VA Commitment by up to 200,000 VAs, reducing the Province Adjusted VA Commitment to 1,300,000 VAs;

(c) the reduction for the STMS Calgary Data Centre in any one Contract Year cannot reduce the Province VA Commitment for the STMS Calgary Data Centre below the greater of:

(i) the maximum Province VA Commitment previously achieved at the STMS Calgary Data Centre up to the time of reduction, less 100,000 VAs; or

(ii) the Province Initial VA Commitment or the Province Revised Initial VA Commitment, as applicable, for the STMS Calgary Data Centre.

For Example in the STMS Calgary Data Centre:

- the Province VA Commitment is 300,000 VAs;
- in Contract Year 8 the Province Additional VA Commitment is 50,000 VAs for a Province Adjusted VA Commitment of 350,000 VAs;
- in Contract Year 9 the Province reduces the Province Adjusted VA Commitment by 50,000 VAs, reducing the Province Adjusted VA Commitment to 300,000 VAs;
- in Contract Year 10 the Province Additional VA Commitment is 200,000 VAs for a Province Adjusted VA Commitment of 500,000 VAs;
- in Contract Year 11 the Province can reduce the Province Adjusted VA Commitment by up to 100,000 VAs, reducing the Province Adjusted VA Commitment to 400,000 VAs;

(d) a reduction will not be permitted until twelve months after the full phase-in of the Province Adjusted VA Commitment.

(e) where the reduction to the Province Adjusted VA Commitment results in the new Province Adjusted VA Commitment falling below a VA Price Row volume band, the VA Unit Price for the new Province Adjusted VA Commitment VAs will adjust to the VA Unit Price associated with the VA Price Row new volume band. For example:

- the Province Adjusted VA Commitment at the STMS Interior Data Centre is 1,750,000 VAs and the VA Unit Price is
- the Province reduces its Province Adjusted VA Commitment to 1,450,000;
- the VA Unit Price for the new Province Adjusted VA Commitment of 1,450,000 VAs will increase to

If the Province requests the Service Provider to expand the STMS Interior Data Centre to accommodate a Province Adjusted VA Commitment of 2,400,000 VAs, then upon acceptance of a Change Order therefor by the Service Provider, the Province Initial VA Commitment or Province Revised Initial VA Commitment, as applicable, will be, and be deemed to be, 2,400,000 VAs for the purposes of any reductions requested by the Province under paragraphs (a) to (e) above in this Section.

If the Service Provider initiates an expansion to the STMS Interior Data Centre without being requested to do so by the Province, then the Province will be entitled to increase its Province Adjusted VA Commitment within the volume range of 1,800,000 to 2,399,999 (and for greater clarification the Province Initial VA Commitment or Province Revised Initial VA Commitment, as applicable, will not be, or be deemed to be, changed to 2,400,000 VAs for purposes of any reductions requested by the Province under paragraphs (a) to (e) above in this Section).

Any reduction to Province Additional VA Commitments must be requested through the Change Order Process. If the Change Order requires changes to Customer Environment(s), then one-time charges to implement the changes, as defined in the Customer Environment Fees section below will apply.

4.11 Extraordinary Reduction to Province VA Commitment

During the periodic reviews set out in the Section 7.2 of the Data Centre SOW, and if requested by the Province through the Change Order Process, the Service Provider may, at its sole discretion, agree to a reduction in the Province VA Commitment to a level below the Province Initial VA Commitment or the Province Revised Initial VA Commitment, as applicable. If such reduction in the Province VA Commitment is approved by the Service Provider, then the VA Unit Price for the new Province Adjusted VA Commitment will be the VA Unit Price associated with the new volume level in the applicable VA Price Row, or such other amount as may be agreed to in the Change Order.

The extraordinary reduction will be requested through the Change Order Process and if it requires changes to the Customer Environment, may result in one-time charges to implement such changes.

4.12 New Data Centre Technology & Impact to Co-location Capacity Reservation

This Section applies to BPS Customers who only purchase STMS Data Centre Services, as described in the Data Centre SOW. If the BPS Customer wishes to make use of new technology, as identified in Section 5.5 (*Data Centre Future Proofing*) of the Data Centre SOW, either because it becomes available at either of the STMS Data Centres as a result of a request made by the BPS Customer or has been initiated by the Service Provider ("**New Technology**"), then:

(a) the Service Provider will provide the BPS Customer with a Change Order, coordinated through the Administrator, that sets forth:

(i) any increase to the existing VA Unit Price related to the use of the New Technology (the amount of the increase to the VA Unit Price being referred to as the "**Unit Price Increase**"), and for greater clarification the Unit Price Increase will be paid by the BPS Customer in addition to the VA Unit Price; and

(ii) either (as determined by the Service Provider):

A. the one-time cost of retro-fitting the BPS Customer's existing Customer Environment (the "**Existing Data Centre Space**") with the New Technology, or

B. the one-time cost of relocating the BPS Customer's Capacity Reservation (or the Adjusted Capacity Reservation, as applicable) from the Customer's Existing Data Centre Space to an area in the same STMS Data Centre with the New Technology (the "**VA New Technology Transfer**"), and any additional costs associated with specific New Technology requested by the BPS Customer that is not otherwise being made available by the Service Provider (the "**New Data Centre Space**");

(b) the VA New Technology Transfer will not increase or decrease the Capacity Reservation (or the Adjusted Capacity Reservation, as applicable) of the BPS Customer, and such Capacity Reservation (or Adjusted Capacity Reservation) will be transferred from the BPS Customer's Existing Data Centre Space to the New Data Centre Space;

(c) notwithstanding the above, and subject to agreement in the Change Order, the BPS Customer may maintain a portion of its Capacity Reservation (or Adjusted Capacity Reservation) at the BPS Customer's Existing Data Centre Space and only move a portion of its Capacity Reservation (or Adjusted Capacity Reservation) to the New Data Centre Space (a "**Partial VA New Technology Transfer**");

(d) the BPS Customer will continue to be charged for the full Capacity Reservation (or Adjusted Capacity Reservation, as applicable) at the BPS Customer's Existing Data Centre Space until the Customer Environment is vacated, or partially vacated in the case of a Partial VA New Technology Transfer, as applicable;

(e) the Unit Price Increase for the use of the New Technology (either in the Existing Data Centre Space or the New Data Centre Space, as applicable) will commence on the Installation Date of the New Technology.

For greater clarification, if the Province increases its Province VA Commitment, then only the VA Unit Price will be decreased and the Unit Price Increase will remain unchanged.

The VA Unit Price will remain unchanged, however a VA technology increase may apply to the VAs that are part of the VA New Technology Transfer and such increase at each VA band will be part of the Change Order.

The Province VA Commitment will still be used to determine when the next VA band is crossed as an Province Additional VA Commitment is added.

4.13 STMS Data Centre Rates

This Section describes the STMS Data Centre VA Unit Prices, the Customer Environment Fees and the Optional Data Centre Services.

4.13.1 VA Unit Prices Summary

The VA Price Tables details the VA Unit Prices based on the various Province Initial VA Commitment or Province Revised Initial VA Commitment scenarios as described in Section 4.6 (*Increases to the Province Initial VA Commitment by June 30, 2009*).

Shortly after the Province finalizes the Province Revised Initial VA Commitment, the Parties will update the VA Price Tables (Tables A, B and C) to include only the VA Price Column associated with the final Province Revised Initial VA Commitment.

The revised tables will resemble Table B(i) where the appropriate range for the VA Price Column header and the Province Adjusted VA Commitment in each VA Price Row will be based on the Province Revised Initial VA Commitment.

4.13.2 Discounted VA Rates for Managed Services

The VAs used in the delivery of Managed Services to the Province will use the VA Unit Prices, discounted by 5% (the "**VA Discount**").

If the BPS Customer purchases any Managed Services from the Service Provider, then the VA Discount will apply only to the VAs reserved by the BPS Customer for the Managed Services so purchased. For greater clarification, the VA Discount will not apply to the VA Unit Price for the VAs reserved by the BPS Customer under its Capacity Reservation (or Adjusted Capacity

Reservation, as applicable) for the "co-location services" purchased by the BPS Customer, as more particularly described in the Data Centre SOW.

4.13.3 Undiscounted VA rates for co-location clients

VAs used for a BPS Customer who only purchase STMS Data Centre Services, as described in the Data Centre Services SOW, uses the VA Unit Prices without the VA Discount applied.

4.13.4 Customer Environment Fees – BPS Customers

This Section applies to BPS Customers. The Customer Environment Fees are for the following (but without duplication of the costs to retro-fit Existing Data Centre Space or to move to New Data Centre Space in connection with the use of New Technology as described in Section 4.12 above):

(a) the Customer Environment set-up and installation during the Capacity Phase-in period;

(b) changes to the Customer Environment required as a result of Additional Capacity Reservations made by the BPS Customer;

(c) changes to the Customer Environment required as a result of any reductions to Adjusted Capacity Reservation made by the BPS Customer; or

(d) reconfigurations to the Customer Environment as requested by the BPS Customer.

There is a one-time Customer Environment Fee for the set-up and installation of the Customer Environment, which is based upon the BPS Customer's requirements for its Customer Environment (such as cage dimensions, cabling trays, fibre builds, network cross connections, cabinets, racks and power circuits). The Customer Environment Fees for the matters referred to in paragraphs (a) to (d) above will be based upon the fees set forth in Appendix B – *STMS Data Centre Price Table*, some of which will be quoted to the BPS Customer at the time of the Change Order for the particular services, and may depend upon custom elements requested by the BPS Customer.

4.13.5 Customer Environment Fees – Province

The one-time Fees for the Customer Environment for the Province are based on:

(a) the Customer Environment set-up and installation during the Capacity Phase-in period;

(b) changes to the Customer Environment required as a result of Province Additional VA Commitment;

(c) changes to the Customer Environment required as a result of any reductions to Province Adjusted VA Commitment; or

(d) reconfigurations to the Customer Environment as requested by the Province.

The Service Provider will define and build the Customer Environments for the delivery of the Managed Services to the Province. The Customer Environment Fee is based upon the requirements for the Customer Environment (such as cage dimensions, cabling trays, fibre builds, network cross connections, cabinets, racks and power circuits). The Customer Environment Fees for the matters referred to in paragraphs (a) to (d) above will be based upon the fees set forth in Appendix B – *STMS Data Centre Price Table*, some of which will be quoted to the Province at the time of the Change Order for the particular services, and may depend upon custom elements requested by the Province.

For budgeting purposes, the Province can multiply the total VAs for a particular Customer Environment by with one rack per 25 square feet and a single overhead basket tray suitable for copper distribution cabling and with one rack per 25 square feet and two overhead basket trays, each suitable for copper distribution cabling or for fibre distribution cabling. The Where the Customer Environment Fee is more than the for one overhead basket tray or for two overhead basket trays, the Service Provider shall explain to the Province the reasons for the differences, and together with the Province will determine a configuration that balances the Customer Environment Fee against the Province requirements. At issue for Inquiry

4.14 Monthly Invoicing

All of the Fees payable by the Province to the Service Provider for the STMS Data Centre Services will be invoiced by the Service Provider to the Province on a monthly basis in accordance with Section 7.3 (*Invoice Timing*) below.

The first month for which the monthly VA Fees will be invoiced to the Province for a given STMS Data Centre will be the month of the Availability Date (as more particularly described in Section 4.4 (*Availability Dates and Province Initial VA Commitment*) for the Province Initial VA Commitment or Province Revised Initial VA Commitment within that STMS Data Centre that has not been allocated to a BPS Customer. For greater clarification, all VAs that are allocated to a BPS Customer will be invoiced directly to the BPS Customer and not to the Province.

The references to the VA Unit Price and to the VAs are based upon a single VA unit, but the Service Provider will invoice the Province on a kVA basis. To convert a volume from VAs to kVAs, and a VA Unit Price to a kVA Unit Price:

(a) VA volumes are divided by 1,000; and

(b) The VA Unit Price is multiplied by 1,000 (the "kVA Unit Price").

For example:

	Volume in VA	Convert to kVA	Volume in kVA
VA Commitment	200,000	Divide by	200.00

	Volume in VA	Convert to kVA	Volume in kVA
		1,000	
VA Unit Price/kVA Unit Price		Multiply by 1,000	
Monthly VA Fees (volume unit price)	At issue for Inquiry		At issue for Inquiry

During the phase-in of the Province Initial VA Commitment or Province Revised Initial VA Commitment (or a Province Additional VA Commitment, as applicable), the monthly invoice will be based on the applicable Province VA Commitment multiplied by the applicable phase-in percentage at a given STMS Data Centre, converted to kVAs, multiplied by the applicable kVA Unit Price for that STMS Data Centre.

For example, where the phase-in has reached 70% at the STMS Interior Data Centre, and the Province VA Commitment is 1,200,000 VAs, then the monthly invoice during that year of the phase-in will be as follows:

- 1,200,000 VAs divided by 1,000 (to convert to kVAs);
- multiplied by 70% = 840.0 kVAs;
- VA Unit Price multiplied by 1,000 (to convert to kVA Unit Price) = kVA Unit Price;
- 840.0 kVAs multiplied by the ‹VA Unit Price = monthly VA Fees of for the relevant phase-in period.

At issue for Inquiry

Once the Province is at 100% of its Province VA Commitment, the monthly invoice will be based upon the applicable Province VA Commitment at the given STMS Data Centre, converted to kVAs, multiplied by the applicable kVA Unit Price for that STMS Data Centre.

For example, where the Province is at 100% of the Province Initial VA Commitment or Revised Initial VA Commitment, or Province Adjusted VA Commitment, as applicable, at the STMS Interior Data Centre, and the Province Initial VA Commitment or Revised Initial VA Commitment (or Province Adjusted VA Commitment) is 1,200,000 VAs, then the monthly invoice for the VA Fees in that year of the phase-in will be:

- 1,200,000 VAs divided by 1,000 (to convert to kVAs);
- multiplied by 100% = 1,200 kVAs;
- VA Unit Price multiplied by 1,000 (to convert to kVA Unit Price) = kVA Unit Price;
- 1,200 kVAs multiplied by the kVA Unit Price = monthly VA Fees of

At issue for Inquiry

4.15 Optional Data Centre Services

The BPS Customers purchasing STMS Data Centre Services from the Service Provider may also purchase the Optional Data Centre Services as described in the Data Centre SOW.

The Service Provider will make available to the Province, as a Managed Services Customer, the following Optional Data Centre Services as described in the Data Centre SOW:

(a) Media destruction – tape;

(b) Media destruction – disk; and

(c) IT equipment disposal.

Appendix B – *STMS Data Centre Price Table* sets forth the Unit Prices for the Optional Data Centre Services.

4.16 WTS Co-location Clients

Within WTS, the Province has a number of Broader Public Sector entities (who are not otherwise BPS Customers) that purchase co-location services from the Province. If these entities remain clients of WTS, then they may purchase STMS Data Centre Services and Optional Data Centre Services through WTS but provided by the Service Provider. The Service Provider will invoice the Province for the STMS Data Centre Services that these Broader Public Sector entities consume.

5. OTHER FEES

The following provides additional information on the characteristics of the other fees not expressly part of midrange, mainframe or storage Unit Prices.

5.1 Milestone Payment

At issue for Inquiry

The Province will pay the Service Provider a milestone payment of (the "**Milestone Payment**") upon the Service Provider's achievement of the Milestone Deliverable. Refer to Schedule 9 (*Transformation SOW*) for details regarding the Milestone Deliverable.

This Milestone Payment will provide funding for both the purchase of the Site (as defined in the Transformation SOW) and for preparing the Site as a data centre for delivery of the STMS Interior Data Centre Services.

When the Milestone Deliverable is achieved, the Service Provider will provide the Province with the Certification (as defined in the Transformation SOW) to confirm that the Milestone Deliverable has been achieved. The Certification will be presented to the Province as part of the invoice for the Milestone Payment on or before March 31, 2009. The invoice is due and payable by the Province in 10 Business Days.

5.2 Month 1 to 6 Fee

The billing from Service Provider to the Province during month 1 to 6 of the Term will not be based on Unit Prices, but instead be based on a fixed monthly charge for the delivery of the Managed Services:

Month	Monthly fixed fee
March 30-31, 2009	
April 2009	
Sub-total April invoice	
May 2009	
June 2009	
July 2009	
August 2009	
September 2009	
TOTAL	

For reporting purposes between the Service Provider and the Province, the March 30 to 31 Fees will be considered part of Contract Year 1.

Material increases to volumes during the month 1 to 6 period shall be invoiced in addition to the month 1 to 6 fee based on the incremental volume multiplied by the applicable Unit Price for the 2009/2010 Contract Year.

5.3 Transformation

5.3.1 Transformation Summary

The Fees for the Transformation Services described in Schedule 9 (*Transformation SOW*) shall be billed to the Province as described in Section 7.3.2 (*Invoicing for the Transformation Fee*). The Fees for the Transformation Service include:

(a) network installation and setup (excluding hardware which is part of the Capital Payment);

(b) mainframe migration and the temporary hardware (but excluding the balance of the mainframe hardware which is part of the Capital Payment);

(c) storage and backup and retention migration;

(d) transformation project management; and

(e) midrange transformation (excluding Initial and Refresh Installs).

5.3.2 Transformation Deliverables

The Managed Services Price Table contains the Fees for the Transformation Services. The Service Provider will perform the Transformation Services, and will complete the deliverables described in Appendix I, at the times set forth in the Transformation SOW; however the Fees for the Transformation Services will be invoiced monthly until the expiry of the Initial Term Managed Services (as defined in the Agreement). See Appendix C – *Managed Services Price Table* for the monthly Fees for the Transformation Services.

5.4 Application Enabling Services (AES)

The Service Provider will provide the Application Enabling Services (AES) if requested by the Province and in accordance with the Application Enabling Services SOW. The Service Provider will invoice the Province for the Application Enabling Services in accordance with the provisions set forth below (including during months 1 to 6 of the Term, as applicable).

5.4.1 AES Level of Effort

The Province agrees to a minimum commitment of 3,900 billable hours per Contract Year for the Application Enabling Services (the "**AES Minimum**"). The AES Minimum may be increased as agreed to by the Parties as part of the Annual Operating Plan. Notwithstanding the foregoing, under no circumstances shall the Service Provider claim for any additional costs set forth in Sections 5.4.2(a) or 5.4.2(b) relating to an increase beyond 11 Service Provider Personnel where the Application Enabling Services have not been increased beyond the AES Minimum.

The Transferred Employees who are performing the Application Enabling Services as Service Provider Personnel previously performed other services and work for the Province, prior to the Effective Date, that was not described in the Application Enabling Services SOW (the "**Non-AES Work**"). The Parties acknowledge that from and after the Effective Date, the Application Enabling Services shall not include any Non-AES Work and the Non-AES Work shall not be, or be deemed to be, the services described under Section 4.2 (*Included or Inherent Services*) of the Agreement.

5.4.2 AES Hourly Rates

The Province will pay hourly rates for the Application Enabling Services (the "**AES Hourly Rates**") for services provided during regular business hours between 08:00 and 17:00 each Business Day, but based on a 7 hour day (which 7 hours day does not include the time taken for a lunch break), as follows:

Category	AES Hourly Rates
Intermediate Analyst	
Senior Analyst	
Technical Specialist	

At issue for Inquiry

The AES Hourly Rates are built-up from salary and include other employee- related costs. The AES Hourly Rates do not include the following:

(a) an allocation of work space for more than 11 Service Provider Personnel to provide the Application Enabling Services (and if more than 11 Service Provider Personnel are required, then it will be subject to a Change Order for the additional work space);

(b) an allocation for Service Provider management personnel if the number of Service Provider Personnel who provide the Application Enabling Services grows beyond 11 people;

(c) an allocation for project management if the number of Service Provider Personnel who provide the Application Enabling Services is involved in a project with a need for project management;

(d) Travel and Living expenses required in conjunction with the Application Enabling Services; and

(e) additional hardware required for a specific Application Enabling Services project (the rate does include the Service Provider Personnel's PC and MS office suite used to provide the Application Enabling Services).

Service Provider acknowledges that the AES Hourly Rates (and AES Hourly Overtime Rates set forth below) may be published in a catalogue that the Province uses with the Client Ministries.

5.4.3 AES Hourly Overtime Rates

Where Service Provider Personnel providing the Application Enabling Services is required to work overtime to complete the services, then the following rates (the "**AES Hourly Overtime Rates**") shall apply:

Category	Hourly Rates for Time and a half	Hourly Rates for Double time
Intermediate Analyst		
Senior Analyst		
Technical Specialist		

At issue for Inquiry

Where the Service Provider Personnel are eligible for the following rates of pay as per the Service Provider Advanced Solutions Collective Agreement, then the following shall apply:

(a) in respect of double time pay as, the AES Hourly Overtime Rates used, and set forth above, are based upon a 50% premium to the regular AES Hourly Rates; and

(b) in respect of time and a half pay, the AES Hourly Overtime Rates used, and set forth above, are the same as the AES Hourly Rates, and no premium will apply.

5.4.4 Changes to the AES Hourly Rates

Service Provider will adjust the AES Hourly Rates and the AES Hourly Overtime Rates every year as per the Section 6.3.1 (*BCGEU Collective Agreement Inflation*).

5.4.5 AES Time Reporting

The Service Provider Personnel performing the Application Enabling Services will enter actual time worked into the Province's "Remedy" electronic time sheet system or other such replacement tool as may be notified by the Province to Service Provider (the "**Time Sheet System**"). The Province will provide the applicable Service Provider Personnel with access to the Time Sheet System where access is available from a Service Provider location. Time entered into the Time Sheet System will be in increments of 30 minutes. Service Provider will be granted the ability to generate reports from the Time Sheet System in order to invoice the Province for the Application Enabling Services provided. Service Provider will have at least two Service Provider Personnel who are able to generate the required reports from the Time Sheet System.

The Province will provide ongoing training for the use of the Time Sheet System as may be reasonably required to enable the Service Provider Personnel performing the Application Enabling Services and the Service Provider Personnel who are generating the reports to enter time into the system and generate the reports.

If the Province is unable to provide the Service Provider with access to the Time Sheet System, then the Parties will work together to determine an alternate means by which the Service Provider will report the actual time spent by the Service Provider Personnel in performing the Application Enabling Services (such as a monthly Excel report that provides the details on the daily hours worked for each resource by project).

5.4.6 AES Invoicing

Service Provider will invoice the Province for the Application Enabling Services at approximately the same time that Service Provider provides invoices for other services to the Province under Section 7.3 (*Invoice Timing*). The invoices for the Application Enabling Services will be based upon the time worked from mid-month to mid-month and entered into the Time Sheet System (and where the Province is unable to provide the Service Provider with access to the Time Reporting System, then as supported by the reporting detailed above). The Province will pay such invoice within 10 Business Days following receipt.

For example, the June invoice would be provided to the Province mid-June for the hours worked from mid-May to mid-June.

5.4.7 AES Minimum Invoicing

At the end of each Contract Year the Parties will calculate the difference between the AES Minimum and the number of hours worked by the Service Provider Personnel in performing the Applicable Enabling Services during that Contract Year (the "**Actual AES Hours**"). If the Actual AES Hours is less than the AES Minimum, then the difference (the "**AES Shortfall**")

will be invoiced by the Service Provider to the Province on the first invoice of the next Contract Year, calculated as follows:

- AES Shortfall (hours) X AES Hourly Rate for a Senior Analyst for the Contract Year in which the AES Shortfall occurs.

5.5 After Hours Service Desk (Optional)

The After Hours Service Desk is a service available to the Province through the Change Order Process.

The monthly Unit Price for the After Hours Service Desk services (which are more particularly described in the Schedule 7 (*Service Management SOW*)) is set forth in Managed Services Price Table. These After Hours Service Desk services will be delivered from the Service Provider Help Desk center in Winnipeg, Manitoba.

The monthly Unit Price for After Hours Service Desk set forth in the Managed Services Price Table is based upon a call volume of 430 calls per month. If the actual call volumes received by the After Hours Service Desk as part of the services are consistently above 430 calls per month, then the fees payable by the Province to the Service Provider for such increased call volumes will be addressed in a Change Order to cover the costs to the Service Provider to adequately staff the After Hours Service Desk.

The Service Provider will invoice the Province for a one-time After Hours Service Desk setup Fee, as set forth in the Managed Services Price Table, when the After Hours Service Desk deliverables that are set forth in Schedule 9 (*Transformation SOW*) are achieved or completed by the Service Provider.

5.6 BC Hydro Rebate

5.6.1 BC Hydro Rebate - Summary

Under the BC Hydro Power Smart Program (which provides subsidies for reducing the power consumption of Server hardware under certain circumstances), the Service Provider will engage a third party to perform an energy study that the Service Provider will submit to BC Hydro for evaluation under the Power Smart Program (an "**Energy Report**"). The Province engaged a third party to prepare an Energy Report on the Wintel Server environment and will share the findings and the Energy Report with the Service Provider after the Effective Date. The Service Provider will use the same or similar third party to prepare the Energy Reports on the other Server environments. The Parties expect that:

(a) the Energy Report will include the power consumption reduction impacts of both the refresh of physical Servers and the virtualization of Servers, and may be prepared in phases through the applicable transformation projects (such as Server virtualization);

(b) BC Hydro will determine the amount of power reduction that is attributable to the Service Provider's transformation plan for Server refresh and Server virtualization; and

(c) where BC Hydro determines that a rebate may be granted, the Service Provider will continue to work with BC Hydro to try to achieve the BC Hydro rebate described below.

5.6.2 Sharing of BC Hydro Rebate

The table below shows the annual expected BC Hydro rebate included in the Service Provider SDO&G (the "**Expected Rebate**"). The annual BC Hydro rebate received by the Service Provider is referred to as the "**Actual Rebate**". The Actual Rebate will fund the cost that the Service Provider incurred for the Energy Report (such cost being offset by any amount of the Energy Report that may be funded by BC Hydro), and the balance of the Actual Rebate (the "**Net Rebate**") will be shared between the Parties as set forth below. The Service Provider will share the BC Hydro decision regarding the Actual Rebate with the Province.

Where the Service Provider receives a Net Rebate that is less than the Expected Rebate, then the Service Provider and the Province will share any shortfall on a 50% / 50% basis. The Service Provider will invoice the Province for half of any such shortfall at the beginning of Contract Year following the year in which the shortfall applies.

Where the Service Provider receives a Net Rebate that is greater than the Expected Rebate, then the Service Provider and the Province will share any excess amount on a 50% / 50% basis. The Service Provider will provide the Province with a credit for half of any such excess at the beginning of Contract Year following the year in which the excess applies.

Fiscal Year	Annual Expected Rebate
11/12	$37,500
12/13	$150,000
13/14	$150,000
14/15	$150,000
15/16	$112,500
TOTAL	$600,000

5.6.3 Annual Report

Commencing in the Contract Year 2012/13, the Service Provider will provide an annual report to the Province that summarizes the Energy Reports produced in the prior Contract Year, submissions to BC Hydro, the BC Hydro Actual Rebate received and variances to the Expected Rebate.

5.7 Other Optional Services (Not Part of Unit Prices)

5.7.1 Optional Security Services

The Province may purchase the following optional security services (which are more fully described in the Schedule 3 (*Security SOW*)) through the Change Order Process:

(a) Two-Factor Authentication (2FA) for Service Provider Privileged Access for Service Provider Personnel providing Services under the Agreement;

(b) Two-Factor Authentication (2FA) for Province Privileged Access for Province Personnel;

(c) Payment Card Industry Data Security (PCI / DSS) compliance services; and

(d) Security Information Management (SIM) / Enterprise Security Event (ESEM) services.

See Appendix H (*Optional Security Services*) for pricing for the optional security services referred to above.

5.7.2 Disaster Recovery and Business Continuity Planning

Disaster Recovery (DR) Plans that are identified in the BCP SOW and that are accepted by the Service Provider as described in Schedule 8 (*BCP SOW*) will continue to be supported by Service Provider. Service Provider will not invoice the Province additional Fees to accept the existing DR plans or to perform the Annual Recovery Exercise except as stated in the BCP SOW.

Development of new DR Plans and Annual Recovery Exercise of the new DR Plans, or enhancing existing DR Plans, will be invoiced on a Time and Material basis as described in the BCP SOW.

Storage Reserve Options for Tier 1, 2 and 3 storage are referenced in Schedule 8 (*BCP SOW*). Unit Prices for these options will be provided through the Change Order Process.

Mainframe DR is included through a third party vendor, as more particularly described in the Mainframe SOW.

5.8 Hourly Rates

Appendix M to Schedule 23 contains a list of hourly rates for the Managed Services being delivered under the Agreement (the "**Hourly Rates**"). These Hourly Rates apply to Managed Services provided by EDS Advanced Solutions Inc.'s employees. The purpose of the Hourly Rates is to provide a basis for the Parties to use when the Province or Broader Public Sector procure Managed Services under the scope of the Agreement that do not otherwise have a Unit Price under the Managed Services Price Table.

The Hourly Rates exclude the AES Hourly Rates, the AES Overtime Hourly Rates and the mainframe hourly rates, each of which are discussed above in this Schedule.

5.8.1 Confidential Rates

The Hourly Rates are for use under the Agreement with the Province and the Broader Public Sector entities who purchase Managed Services under a BPS Services Agreement and are not meant for general publication or distribution outside of the Province (EHS) or similar organization of the applicable Broader Public Sector entities. The Province will treat the rates as confidential and limit the distribution to a "need to know" basis, informing Service Provider before providing the rates to anyone outside the Broader Public Sector entities who have a need to know in connection with the Services.

5.8.2 Hourly Rate Build-Up

The Hourly Rates are built-up from salary and include other employee- related costs. The Hourly Rates do not include the following, which will be included through the Change Order Process, as applicable:

(a) an allocation of work space in the event that additional space is required by Service Provider to deliver a project;

(b) an allocation for Service Provider management personnel and project management for a project;

(c) Travel and Living expenses required in conjunction with the project; and

(d) additional hardware required for a specific project (the rate does include the Service Provider Personnel's PC and MS office suite used in the project).

5.8.3 Changes to the Hourly Rates

Service Provider will calculate rates every two Contract Years to account for inflation and market conditions.

5.9

5.10 Cost Responsibilities

Set forth below are the responsibilities of the Province and the Service Provider for certain cost-related matters related to the Managed Services to be provided under the Agreement.

5.10.1 Security Compliance on Initial Supported Infrastructure

The Service Provider will implement remediation plans to address security compliance on the Initial Supported Infrastructure, as requested by the Province pursuant to the provisions of Section 2.1 (*Security Policy Control Standards Compliance*) of the Security SOW, in accordance with the Change Order Process.

5.10.2 Mainframe IP

The mainframe migration transformation fee set forth in the Managed Services Price Table includes establishing some Service Provider Intellectual Property (IP), and the Province providing some of the existing mainframe IP to Service Provider.

Service Provider will receive the following mainframe IP from the Province for use in delivering the Mainframe Services to the Province:

(a) 100% of S15 S15 applications that Service Provider will manage

(b) 50% of reporting code, where the number of reports is 103 out of a total of 207 (as listed in Appendix B of Schedule 4 (*Managed Mainframe SOW*))

Service Provider will produce the following mainframe IP for use in delivering the Mainframe Services to the Province:

(c) 50% of reporting code, where the number of reports is 104 out of a total of 207 (as listed in Appendix B of Schedule 4 (*Managed Mainframe SOW*)) and where Service Provider's Fee is based on the receipt of copies of the existing reports and any specifications for unusual calculations from the Province by June 2010.

(d) 175 tasks for software exits and user mods for Mainframe System Software as defined in the Mainframe SOW. Service Provider's Fee is based on the receipt of specifications from the Province by June 2010 and the following breakdown of complexity, where complexity is determined by specification verification, coding, testing and integrated testing.

(i) 75% of tasks will be simple – average of 8 hours to complete

(ii) 16% of tasks will be easy – average of 40 hours to complete

(iii) 6% of tasks will be medium difficulty – average of 80 hours to complete

(iv) 3% of tasks will be complex – average of 160 hours to complete

The Parties will discuss changes to the development of the mainframe IP requirements and where the Parties determine that the effort required to develop the mainframe IP is different than as set forth in paragraphs (c) and (d) above, or where changes to paragraphs (c) or (d) occur after June 2010, the Parties will discuss a Change Order.

5.10.3 Service Provider use of Province Assets

The Province will allow Service Provider the use of the following Province assets, without charge to Service Provider, solely for the purpose of providing the Managed Services under the Agreement:

(a) the Province Data Centres, Regional Network Centres and Remote Sites (all as defined in the Server Management Services SOW);

(b) the Initial Supported Infrastructure (as defined in the Security SOW);

(c) all of the Use Rights granted to Service Provider under the Master Transfer Agreement (which includes the software licenses, software support agreements, hardware maintenance agreements listed in, a Schedule to the Master Transfer Agreement in respect of the Supported Infrastructure);

(d) the software listed in Schedule 14 (*Software Responsibility Table*) as being the responsibility of the Province;

(e) all network circuits used for Service Provider to deliver the Managed Services are the responsibility of the Province. Specifically, the network circuits are expected to be:

(i) S15 STMS Data Centre; and

(ii) S15 STMS Data Centres;

(f) the Province may request the Service Provider to procure the network circuits into the STMS Calgary Data Centre and the STMS Interior Data Centre through the Change Order Process S15

S15

The Change Order will indicate the cancellation notification period required by the Province.

(g) any Network carrier installation cost (commonly referred to as "last mile" cost) that may be required for the network carrier to connect the circuits the STMS Data Centres (refer to Schedule 2 (*Data Centre SOW*) for details on Service Provider' responsibility to manage the network circuits) is the responsibility of the Province;

(h) until such time that the Transferred Employees relocate from the Province facilities to the Service Provider facilities, which is expected to occur on or about June 30, 2009, the Province shall continue to be responsible for the following costs associated with Service Provider providing the Managed Services from the Province premises:

(i) office facilities, including lease cost, facilities operating cost, furniture, maintenance of building access cards and keys, access to photocopiers and printers, and other similar office equipment;

(ii) computer equipment with continued access to the appropriate tools and software to provide the Managed Services;

(iii) telephones with access to outbound calling for local and long distance calls; and

(iv) any other premises costs associated with having the Transferred Employee on the Province premises;

(v) the matters referred to in clauses (i) to (iv) above as they apply to the Service Provider Personnel hired to provide the Managed Services to the Province who are temporarily located in the Province facilities.

The Parties acknowledge that with the exception of the Microsoft premier support agreement referred to in the Server Management Services SOW, and the software listed in Schedule 43 (*Software Responsibility Table*) as being the responsibility of the Service Provider, the Service Provider is not required to obtain and pay for software support unless otherwise agreed to through the Change Order Process. The Service Provider is not responsible for obtaining and paying for hardware maintenance agreements on the Initial Supported Infrastructure (as defined in the Security SOW), unless otherwise agreed to through the Change Order Process. For greater clarification, it is the responsibility of the Service Provider to pay for any maintenance agreements determined necessary by the Service Provider on any new hardware purchased by the Service Provider after the Hand-Over Date in order for the Service Provider to perform the Managed Services under the Agreement and to otherwise achieve the Service Levels.

(i) **Secure Shipment of Media**

The Province will continue to be responsible for the cost of secure shipment of replacement parts for break/fix activities and media to be destroyed to or from WTS Remote Sites. The Parties will establish an annual cap on the service of The Province will notify Service Provider when the cap is reached and the Parties will discuss the matter through Governance.

At issue for Inquiry

Service Provider will make the shipping arrangements directly with the Province's selected vendor, currently BC Mail Plus.

5.10.4 Basic Infrastructure Credit

As per Section 20.10 (*Basic Infrastructure Credit Payment*) of the Agreement, if Service Provider is required to pay a Basic Infrastructure Credit, then there will be a Change Order issued which will account for changes in Service Provider's cost, if applicable.

6. FEE ADJUSTMENTS

6.1 Work-in-Progress Projects

The Parties acknowledge that the Service Provider established the Fees for the Managed Services to be provided under the Agreement on the basis that there would be no one-off work-in-progress (WIP) projects that exist as of the Hand-Over Date (and for greater clarification, the WIP does not include the ordinary course cycles of Managed Services that are specifically described in the SOWs).

Any WIP that the Service Provider is required to complete will be handled through a Change Order. Any material changes to the scope of work handled by the Transitioning Employees or to the manner that the services are delivered by Service Provider to the Province as a result of the WIP projects will be handled through a Change Order.

6.2 Project work

Project work that is not part of the Transformation Fees will be handled through the Change Order Process (and for greater clarification, services that can be ordered through the Province Ordering System is not considered by the Parties to be "project work").

6.3 Managed Services Inflation

The Unit Prices in the Managed Services Price Table are valid until March 31, 2010. The first application of inflation will take place on April 1, 2010. This section describes how inflation will be applied to the Unit Prices in the Managed Services Price Table.

6.3.1 BCGEU Collective Agreement Inflation

The Province's BCGEU Collective Agreement inflation (as described more fully below) shall be applied to the following Unit Prices (or components of the Unit Prices) in the Managed Services Price Table (and for Unit Prices not listed below, if the support is primarily provided by EDS Advanced Solutions Inc., then the Parties agree that BCGEU Collective Agreement inflation will apply):

(a) Server Management Services Unit Price components (for both physical Servers and Virtual Servers)

  (i) Management Services,

  (ii) Pager Support,

  (iii) Cluster Management,

  (iv) Remote field services;

(b) other midrange Unit Prices:

(i) Shared File and Print Services,

(ii) Shared Database Services,

(iii) Shared Web Hosting Services,

(iv) Initial Server Installations,

(v) Refresh Server Installations,

(vi) Citrix Server Support,

(vii) Dedicated Web Services – Optional,

(viii) Optional Midrange Services (see Section 2.3.8 (*Optional Midrange Services*),

(c) Managed Storage, Backup and Extended Retention Unit Price for the support component;

(d) Optional Storage Services Unit Prices (see Section 2.5.4 (*Optional Storage Services*);

(e) AES Hourly Rates and AES Hourly Overtime Rates.

6.3.2 Application of the Province's BCGEU Collective Agreement Inflation

Service Provider shall be entitled to receive increases in the above listed Unit Prices (and components of the Unit Prices) set forth in the Managed Services Price Table as a result of the application of the Province's BCGEU Collective Agreement inflation as follows:

(a) the provisions of this section shall apply with respect to each increase in compensation agreed to by the Province and the BCGEU under the Province's Collective Agreement. For the purposes of this section, "increase in compensation" includes salary increases, including TMA (Temporary Market Adjustment) increases, one-time or on-going bonus payment, or other payments made by the Province to the employees who are members of the BCGEU, wage adjustments, increases in fringe/benefits (such as dental, medical), pension increases or other increases given in lieu of salary increases that impacts total compensation or payments made by the Province to the employees who are members of the BCGEU (but without duplication of Section 6.7.2 (*Pension Adjustment*) below). For the purposes of the inflation calculation, increases to vacation entitlement, or other such paid leave, shall also be considered an "increase to compensation";

(b) with respect to each such increase referred to in paragraph (a) above (the "**BCGEU Inflation**"), the Parties shall agree on the calculation of the percentage increase (the "**Percentage Increase**") to be made to the Unit Prices (and

components of the Unit Prices) referred to in Section 6.3.1 (*BCGEU Collective Agreement Inflation*) above to account for the BCGEU Inflation. See below for guidance on calculating the Percentage Increase;

(c) if there is no BCGEU Inflation, or if there is negative BCGEU Inflation, then there shall be no decrease in the Unit Prices (and components of the Unit Prices) referred to in Section 6.3.1 (*BCGEU Collective Agreement Inflation*) above. If negative BCGEU Inflation occurs, see Section 6.3.4 (*Negative BCGEU Inflation*) below for additional information.;

(d) once the Percentage Increase has been calculated, the Percentage Increase so calculated shall be applied to the Unit Prices (and components of the Unit Prices) referred to in Section 6.3.1 (*BCGEU Collective Agreement Inflation*) above by multiplying the then-current Unit Price or Unit Price component as applicable with (1 + Percentage Increase):

- For example, if the Unit Price is $85.46 , and if the Percentage Increase is 2.4%, then $85.46 * (1+.024) for a new Unit Price of $87.51.

6.3.3 Guidance on Calculating the Percentage Increase

The Parties acknowledge that the BCGEU Inflation may be based upon one or more of the following inflationary components:

(a) a percentage change to base salary, referred to below as (the "**Percentage Salary Change**");

(b) a base salary increase (where expressed as a dollar amount and not a percentage);

(c) a non-base salary impact (such as bonus, Temporary Market Adjustment); and

(d) A non-salary impact (such as vacation allowance, pension, dental and medical).

Step 1: To convert (b) to (d) to a percentage of base salary, the Service Provider will determine a salary baseline based upon the following:

(a) the current Service Provider Personnel providing the Managed Services under the Agreement who are members of the BCGEU (the "**BCGEU Employees**"); and

(b) the monthly salaries of the BCGEU Employees (excluding any TMA) as of March, annualized for a 12 month period (the "**Salary Baseline**"). For example, if inflation is being calculated for Province fiscal year 2011/2012, the Salary Baseline is based on salaries at March 2011.

Step 2: For each component of the BCGEU Collective Agreement, (the "**Component**"), the Service Provider will calculate the annual impact for the effected BCGEU Employees.

Step 2a: Where the Component is a non-salary change, then the Service Provider will determine if the Component has a material impact to Service Provider. If Service Provider determines the impact to be material, Service Provider will estimate the annual cost impact of each Component. If Service Provider determines the impact of the Component to be immaterial, then the Service Provider will not include the Component in that Contract Year's inflation. If Service Provider determines that the Component is immaterial in one Contract Year, that does not preclude Service Provider from including an estimated impact in a subsequent Contract Year's inflation calculation.

Step 3: For each Component, take the results of Step 2 and divide by the Salary Baseline (each a "**Percentage Component Change**").

Step 4: To calculate the Percentage Increase, add the Percentage Salary Change plus all of the Percentage Component Changes.

6.3.4 Negative BCGEU Inflation

The Parties agree that in Contract Year's where the BCGEU Inflation is negative then future Contract Years BCGEU Inflation must offset the negative BCGEU Inflation before the Service Provider is entitled to an increase to the Unit Prices (and components of the Unit Prices) referred to in Section 6.3.1 (*BCGEU Collective Agreement Inflation*) above.

For example,

- if in Contract Year 4, the BCGEU Inflation is -1.4%, then the Percentage Increase is zero, and
- if in Contract Year 5, the BCGEU Inflation is +2.1%, then the Contract Year 5 BCGEU Inflation is +2.1% - 1.4% = 0.7% and the Percentage Increase is 0.7%.

6.3.5 BC CPI Inflation

The Province of British Columbia Consumer Price Index ("**BC CPI**") inflation shall be applied to the following Unit Prices (or components of the Unit Prices) in the Managed Services Price Table (and for Unit Prices not listed below, if the support is primarily provided outside of the Service Provider's organization, or if the rate is primarily non-support/effort based, then the Parties agree that BC CPI inflation will apply):

- Hardware, Software and Installation (including maintenance)
- Mainframe (processing, DASD, tape and mainframe optional services)
- Transformation (excluding financing costs)
- After Hours Service Desk

- Service Delivery Ops and Governance component of (i) the Unit Prices and (ii) the Volume Band Adjustment. For greater clarification, inflation is not applied to the unit price adjustment component of either the Unit Price or the Volume Band Adjustment

6.3.6 Application of the BC CPI

Service Provider shall be entitled to receive increases in the Unit Prices (and components of the Unit Prices) referred to in Section 6.3.5 (*BC CPI Inflation*) above as follows:

1. If the BC CPI is at December 31 in any year higher (the "**Current Index**") than the BC CPI one year prior thereto (the "**Base Index**") then the Service Provider Fees shall be increased by:

   Multiplying the then-current Unit Price with (1 + percentage increase), where the Current Index less the Base Index is the percentage increase.

   - For example, if the Unit Price is $51.40 per unit per month, and if the BC CPI has increased by 2.1%, then $51.40 * (1+.021) for a new Unit Price of $52.48 per unit per month.

2. If the BC CPI in paragraph 1 above is negative, there shall be no decrease in Service Provider's Fees.

3. BC CPI is located through the Statistics Canada web site (as at February 2009: http://www40.statcan.ca/l01/cst01/econ09k-eng.htm). Refer to Appendix E to Schedule 23 for screen shot of the website.

If this index should be discontinued or significantly altered, the Service Provider working with the Province will select the replacement index or a suitable, similar index which address British Columbia inflation. Refer to Appendix E (*BC CPI and Data Centre CPI Instructions*) for the Statistics Canada report numbers.

6.3.7 Optional Security Services Inflation

The optional services pricing described in Section 5.7.1 (*Optional Security Services*), like the Managed Services Price Table, includes 2009 inflation. For optional services that start after April 1, 2010, the inflation from April 1, 2010 up to the point in time that the project starts shall be applied to the price and continue as per Section 6.3 (*Managed Services Inflation*) for the balance of the project or Term, as applicable.

6.4 STMS Data Centre Inflation

Appendix A – *VA Price Tables* and Appendix B – *STMS Data Centre Price Table* set forth the prices for STMS Data Centre Services (the "**STMS Prices**") for the period ending March 31, 2012. Inflation will be applied to the STMS Prices commencing in contract month 37 (April 2012).

6.4.1 Data Centre Consumer Price Index

The Consumer Price Index applied to the STMS Prices ("**Data Centre CPI**") is as follows:

(a) for the STMS Interior Data Centre, the percentage change in the Consumer Price Index (Vancouver, B.C., All Items) for the preceding year will apply to STMS Prices applicable to the STMS Data Centre Services provided at or from the STMS Interior Data Centre; and

(b) for the STMS Calgary Data Centre, the percentage change in the Consumer Price Index (Calgary, Atla, All Items) for the preceding year will apply to STMS Prices applicable to the STMS Data Centre Services provided at or from the STMS Calgary Data Centre.

6.4.2 Application of Data Centre CPI

The Service Provider shall be entitled to receive increases in the STMS Prices as follows:

(a) if the applicable Data Centre CPI is a positive number on December 31 in any year, then the applicable STMS Prices will be increased, with effect as of the following April 1, by:

(i) multiplying the then-current STMS Prices for the applicable STMS Data Centre by (1 + the applicable Data Centre CPI), and rounding the resulting number to the same precision (of two or three decimals, as applicable) as the then-current price. For example:

- If the VA Unit Price is and the Data Centre CPI for the STMS Interior Data Centre is 2.4%, then (1+.024) =the new VA Unit Price of $0.661.

At issue for Inquiry

(ii) for greater clarification, the first adjustment to the STMS Prices will take place using the Data Centre CPI at December 31, 2011 and the adjustment will be effective as of April 1, 2012;

(b) if the Data Centre CPI is negative on December 31 in any year, then there will be no adjustment to the STMS Prices; and

(c) the Data Centre CPI is available at the Statistics Canada web site (as at February 2009: http://www40.statcan.ca/l01/cst01/econ45a-eng.htm). Refer to Appendix D – *Data Centre CPI* for screen shot of the website.

If these Data Centre CPIs are discontinued or significantly altered, then the Service Provider working with the Province will select the replacement index or a suitable, similar index which address the Vancouver, British Columbia inflation and the Calgary, Alberta inflation. Refer to Appendix E (*BC CPI and Data Centre CPI Instructions*) for the Statistics Canada report numbers.

6.4.3 Annual Inflation Estimates and Final Inflation Calculation

The Parties will estimate inflation that will apply to the next Contract Year (up to two times a year (the "**First Inflation Estimate**" and the "**Second Inflation Estimate**") with the final inflation calculation happening for April of each year (the "**Final Inflation Calculation**").

6.4.4 First Inflation Estimate

In May of each year, Service Provider will submit a First Inflation Estimate which will estimate the inflation for the following fiscal year (i.e. if the date is May 2010, then the First Inflation Estimate is for the April 2011 to March 2012 period).

Step 1: The First Inflation Estimate will be based on the available information (existing Province BCGEU Collective Agreements as described in Section 6.3.1 (*BCGEU Collective Agreement Inflation)*, if available, or an estimate of upcoming Province BCGEU Collective Agreements if the Province BCGEU Collective Agreement is scheduled for renewal, or the appropriate CPI index as described in Section 6.3.5 (*BC CPI Inflation*).

Step 2: The Parties will discuss the inflation percentage collected from the various sources in Step 1 and determine if an adjustment upwards or downwards is required to more accurately estimate the inflation in the next April to March period.

Step 3: For purposes of Province budgeting, the Service Provider will provide the Province with an updated Managed Services Price Table and VA Unit Price Tables with the estimate of inflation for the upcoming Contract Year.

6.4.5 Second Inflation Estimate (Optional)

The Second Inflation Estimate is an optional estimation exercise and the Parties will determine at the beginning of the year whether the Second Inflation Estimate will be required. If the inflation indices seem to be stable, the Parties will agree that the Second Inflation Estimate is not required. If the Second Inflation Estimate is required then, in September the Service Provider will submit a Second Inflation Estimate which may revise the First Inflation Estimate for the upcoming Contract Year. To conduct the Second Inflation Estimate, repeat the same Steps 1 to 3 from above.

6.4.6 Final Inflation Calculation

In February of each year, Service Provider will submit a Final Inflation Calculation which will be used to update the following for the upcoming Contract Year:

(a) Managed Services Price Table;

(b) VA Price Tables;

(c) AES Hourly Rates and AES Overtime Hourly Rates;

(d) Volume Band Adjustment Tables; and

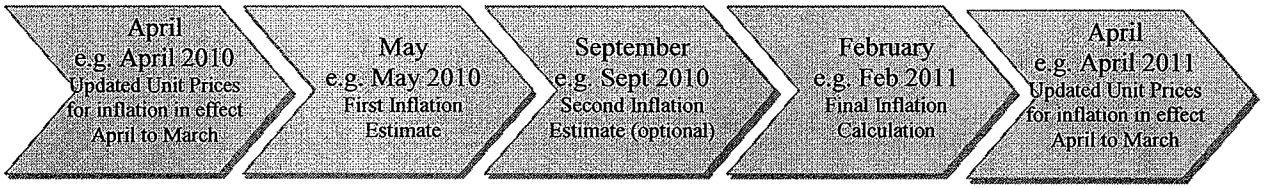
(e) STMS Data Centre Price Table.

For greater clarification, neither the BCGEU Inflation or the BC CPI Inflation is added to the unit price adjustment component of certain Unit Prices.

Step 4: The Final Inflation Calculation will be based on the same information sources as Step 1 above, updated for the prior January to December period (if the date is February 2011, then the period of January to December 2010 is used for CPI based indices).

Step 5: Service Provider will use the Final Inflation Calculation to update (a) to (e) above for the remaining Contract Years and the Unit Prices will apply for the next Contract Year. The updated tables in (a) to (e) will replace any previously published price tables and will become effective on April 1 of the upcoming Contract Year.

6.4.7 Summary of Inflation Estimates and Final Inflation Calculation



6.5 Price Table Changes

Changes to the VA Price Tables, STMS Data Centre Price Table, the Managed Services Price Table (other than changes resulting from inflation as described above) will be made pursuant to the Change Order Process.

6.6 Services Catalogue

The current year's Unit Prices from the Managed Services Price Table, VA Price Table and Data Centre Price Table, as adjusted for inflation, are used to create the annual Managed Services and STMS Data Centre Services Catalogues for the Broader Public Sector entities. The Services Catalogues will be updated by March 1st of each Contract Year. For the first Contract Year, the Services Catalogue will be completed by April 15. A draft of the Services Catalogue is attached as Appendix J (*Services Catalogue*).

6.7 Other Fee Adjustments

6.7.1 Ministry Explicit Agreements

The Managed Services Price Table does not include any consideration for the Ministry Explicit Agreements. Ministry Explicit Agreements not described in the Managed Services SOWs shall be addressed through the Change Order Process.

6.7.2 Pension Adjustment

When the next actuarial valuation of the Public Sector Pension Plan is performed (currently scheduled for March 2011, and such valuation will come into effect March 2012), any adjustment to the employer contribution rate (the components of the current employer contribution rate being set out in the table below), either by way of lump sum or by month, shall result in an adjustment to the Midrange Service and Managed Storage Services Unit Price, more specifically the "Management Services" component of the Unit Price. For the purposes of determining the amount of the adjustment to the Unit Prices, (i) the employer contribution rate used to calculate the adjustment shall be the employer contribution rate resulting from the March 2011 actuarial valuation; (ii) the adjustment shall be determined with respect to all Service Provider employees who are members of the Public Sector Pension Plan and deliver the Managed Services under the Agreement; and (iii) the adjustment shall be applied to the period from the effective date of the new employer contribution rate to the end of the Term.

Pension changes that result from actuarial valuations, other than the actuarial valuation scheduled for March 2011, shall not result in any further adjustment to the Unit Prices.

For example, the current employer contribution rate is 8.78% of earnings up to the YMPE ($44,900 in 2008) plus 10.78% of earnings in excess of the YMPE. If the employer contribution rate increases by 1% for earnings up to YMPE and 1.5% for earnings in excess of YMPE, as a result of the next valuation, then the Unit Prices are increased by the amount of the monthly PSPP increase. The monthly PSPP increase is calculated based on the actual monthly earnings at the point in time that the Public Sector Pension Plan implemented the change in the employer contribution rates through to the end of Term.

A sample calculation at the time of a change in the employer contribution rate is set out below. Sample amounts (other than with respect to the current employer contribution rates which are actual rates at the Effective Date) have been used.

	Earnings up to YMPE	Earnings in excess of YMPE	Total Cost
Monthly Earnings	$1,000,000	$450,000	
Current Employer Contribution Rate	8.78%	10.78%	
New Employer Contribution Rate	9.78%	12.28%	
Employer Contribution Rate Change	1.0%	1.5%	
Increased Monthly Cost	**$10,000**	**$6,750**	**$17,750**

If at the next actuarial valuation described above the employer contribution is decreased, then the same exercise will occur, but a decrease to the Unit Prices as indicated above will result.

7. METHOD OF PAYMENT

7.1 Province Payments

The Province will pay invoices within 10 Business Days of receipt of the invoice from the Service Provider. The Province may dispute any invoice within the times referred to in Section 15.6 of the Agreement.

Subject to the provisions of Section 15.6 of the Agreement, for payments received after the 10 Business Day period, the Province will pay interest on the outstanding amount for the entire month(s) in which payment is delayed at a rate equal to Prime plus 1.5% per annum, where Prime is defined as the prime rate of the Province of British Columbia's principal banker, currently CIBC, compounded as set forth below. For example, if a payment is received 5 days after the expiry of the 10 Business Day due date, the first month's interest calculation is:

- Amount of invoice not paid multiplied by interest rate divided by 12 months.

Subject to the provisions of Section 15.6 of the Agreement, if the overdue amount is still outstanding 30 days after the due date, then interest is calculated on the amount of the invoice not paid plus outstanding interest. Interest is calculated for each 30 day period that the overdue amount is outstanding until the invoice and interest is paid in full.

7.2 Payments from the Broader Public Sector

The Managed Services Price Table, VA Price Tables and the STMS Data Centre Price Table are based on the method of payment described in this Section. If a Broader Public Sector entity does not wish to follow the payment terms as described, then:

(a) the Parties shall attempt to agree to different payment terms so long as the payment terms are no longer than (i) Service Provider invoicing at the beginning of the month following delivery of services and (ii) the Broader Public Sector paying such invoice in no more than 30 calendar days; and

(b) the Managed Services Price Table, VA Price Tables and STMS Data Centre Price Table being increased to include a 1.5% price increase as a result of the extended payment terms described in paragraph (a).

7.3 Invoice Timing

7.3.1 Invoicing for the Month 1 to 6 Fixed Fee

The invoices from the Service Provider to the Province will be mid-month (approximately the 15th of the month) for the month in which services are provided and will be based on the month 1 to 6 fees in Section 5.2 (*Month 1 to 6 Fee*). The first invoice shall also include the fees associated with March 30th and 31st. Therefore the first invoice shall be for the period March 30 – April 30 and be invoiced approximately mid-April.

7.3.2 Invoicing for the Transformation Fee

Service Provider shall invoice the Province for the Transformation Fee approximately the 15th of each month starting the first month for which Managed Services are provided and will be based on the monthly Transformation Fee in the Managed Services Price Table. The Transformation Fee will continue for the Initial Term Managed Services.

7.3.3 Invoicing for Balance of Contract (Month 7 Onward)

Commencing contract month 7 onward, the Service Provider will invoice the Province for Managed Services based on volumes and Unit Prices on approximately the 15th of each month for the Fees for that month.

The Service Provider will invoice the Province on approximately the 15th of each month for the Fees for that month associated with the STMS Data Centres subject to Section 4.14 of Schedule 23.

7.3.4 Invoicing and Payment Terms for Change Orders

The invoicing and payment terms for Change Orders not based on the Managed Services Price Tables, the VA Price Tables or the Data Centre Price Table shall be:

(a) if the Change Order is deliverable based and the deliverable approval from the Province is attached to the invoice, the invoice shall be paid in 10 Business Days;

(b) if the Change Order is T&M based, the Province shall pay in 30 calendar days; and

(c) anything not identified above, the Province shall pay in 30 calendar days.

7.3.5 Volumes for Invoicing

Through the inventory process defined in Schedule 7 (*Service Management SOW*) section of the Transition SOW, the Parties will work together to determine the quantities, types and other services required for the invoicing of the Managed Services. The monthly invoicing from contract month seven and onward shall be based upon the Unit Prices multiplied by the applicable quantities and taking into account volumes changes processed through the Province Ordering System.

7.3.6 Midrange Services Invoicing

Midrange Services invoicing will be based on the volumes in service on the 15th of the month in Service Provider's Asset Centre. There shall be no pro-ration of a unit put into service after the 1st of the month, but before the 15th, just as there shall be no pro-ration on the next invoice for a unit that was put into service after the 15th of the month. For a unit put into service after the 15th of the month, the first month of invoice for such unit shall be on the next invoice.

For a unit removed from service prior to the 15th, the unit shall not appear on the invoice and there shall be no pro-ration of the unit on the invoice. For a unit removed from service after the 15th, there shall be no pro-ration of the unit and a full month of service shall be invoiced for the removed unit. The first month that the removed unit is no longer on the invoice from Service Provider to the Province is on the following invoice.

By way of example:

Where month in example is month 12	ADDED to service	Invoice on 15th of month 12	Invoice on the 15th of month 13		REMOVED from service	Invoice on 15th of month 12	Invoice on the 15th of month 13
Service Date of unit							
1st to 15th of month 12	X	Yes	Yes		X	No	No
16th to 30th of month 12	X	No	Yes		X	Yes	No

The Parties agree that the purpose of using the unit in service at the 15th of the month is to avoid the administrative burden of pro-rating billable units. The Parties agree not to attempt to add or remove units in a way that systematically benefits one Party to the detriment of the other. The expectation is that additions and removals will occur throughout the month with no pre-disposition to being at any particular point in the month.

Shared Database Services and Shared Web Hosting Services volumes may not reside in Service Provider's Asset Centre in which case the repository will be determined in the month 1 to 6 period. The invoicing will detail the unique identifier of each Shared Database instance and Shared Web site.

Shared File Print Services volumes are based on the users of SFP Services in the Province's Corporate Accounting System (CAS) (more specifically, the records reside within the "Install Base" at the Hand-Over Date). Service Provider will use the Province's information from CAS to determine the number of SFP users. The Province will provide Service Provider with the SFP volumes on the 14th of each month which will appear on that month's invoice. If the Province does not provide the Service Provider with the SFP volumes by end of day of the 14th, then Service Provider will use the previous month's SFP volumes for the current invoice and reconcile any difference on the following invoice once the actual volumes are received.

Where there is incremental SFP storage above the 1.5 GB such incremental SFP storage does not appear in CAS. The Service Provider will provide a SFP storage report that shows the actual Tier 2 storage volume on which the invoice for the incremental storage is based. Refer to Section 2.3.1 (*Shared File and Print Services*) for additional information regarding SFP.

7.3.7 Storage, Backup and Extended Retention Invoicing

Refer to Section 2.5.1 (*Managed Storage (Tier 1, 2, 3, and NAS)*), for Managed Storage invoicing volume information. Managed Storage is invoiced based on a volume of allocated GBs in place on the 15th of the month. The invoice will include the allocated GB by Server name.

Backup and Extended Retention volumes are based on actual usage based on the number of GBs.

The Managed Backup invoicing will be based on the GBs written between the 14th and the 13th each month and such total volume will appear on the invoice generated approximately the 15th of the month. A Managed Backup report will detail the actual usage for that period. The invoice is based on the total backup GBs multiplied by the then-current Unit Price.

The Extended Retention invoicing will be based on the GBs retained on the 13th of each month and such total volume will appear on the invoice generated approximately the 15th of the month. An Extended Retention report will detail the retained GB for that period. The invoice is based on the retained GBs on the 13th multiplied by the then-current Unit Price.

7.3.8 Invoicing of Managed Storage and Managed Backup Services in Thousands of GB

The references to the Storage, Backup and Extended Retention Unit Prices and volumes are based on GBs, but the Service Provider will invoice the Province in thousands of gigabyte ('000 GB). This conversion is solely for the purpose of facilitating the invoicing.

To convert a volume from GBs to '000 GBs, and a GB Unit Price to a '000 GB Unit Price:

- GB volumes are divided by 1,000; and
- The GB Unit Price is multiplied by 1,000 (the "**'000 GB Unit Price**").

For example:

	Volume in GB	Convert to '000 GB	Volume in '000 GB
Storage Volume	157,287	Divide by 1,000	157.287
GB Unit Price/'000 GB Unit Price	At issue for Inquiry	Multiply by 1,000	At issue for Inquiry
Monthly Storage Fees example (volume * Unit Price)			

7.3.9 Mainframe Invoicing

As discussed in Sections 2.4.2 (*Mainframe Processing*) and 2.4.4 (*DASD*), MIPS and DASD volumes are invoiced based on an installed volume basis.

Tape volume is based on actual usage for the number of GBs written per the "tape management catalogue" controlled by the Province's third party provider "removable media manager" software, or other such product as determined by Service Provider.

The monthly invoice volume will be based on:

(a) the sum of the daily, actual GB tape volume per the tape management catalogue from the 14th to the 13th of each month;

(b) the sum in (a) divided by the number of days used in the sum in (a); and

(c) the result of (b) is the average daily GB usage for tape as is multiplied by the then-current Unit Price for tape to produce the amount to invoice.

7.3.10 Province Verification of Service Provider Invoices

The Province will compare the Service Provider's invoice with records

where the Province records do not match the Service Provider's invoice, the Parties will work together to determine the reason for the discrepancy between the records and Service Provider's billing records. For example, a unit recently put into service may not yet be reflected in the records, or vice versa (a timing difference). Where the difference is more than a timing difference, the Parties will work together to resolve the mismatch by either updating the records or Service Provider's billing records based on the outcome of the investigation.

Where the Parties, working cooperatively, are not able to determine the reason for the record's mismatch prior to processing the Service Provider's invoice, the Province may reduce the amount paid to the Service Provider by only by the amount of the mismatch. The Service Provider's invoice is still due in 10 Business Days as described in Section 7.1 (*Province Payments*) above.

The Parties will have a designated person whose responsibility it is to work with the other Party in resolving these billing differences. If the designated persons cannot resolve the issue within 15 Business Days, they will escalate the issue through the Governance process.

The following volumes are not part of the records (see the section above for information on the invoicing backup):

- Shared File Print incremental storage (storage above the 1.5 GB per use on an aggregate Ministry basis)
- Backup
- Extended Retention
- Mainframe – MIPS Processing, DASD and Tape

For details, see the relevant sections above.

8. MARGIN CAP

The point at which the Parties will share the Service Provider profit above a certain Service Provider Margin is (the "**Margin Cap**"). The Margin Cap is expressed as a percentage and changes based on the Annual Growth in Fees in the current Contract Year.

8.1 Service Provider Margin Calculation

The "**Service Provider Margin**" is calculated on a cumulative basis from the Effective Date as follows:

(cumulative Service Provider Revenue – cumulative Service Provider Cost) / cumulative Service Provider Revenue

The Fees invoiced to the Province and any Broader Public Sector entity for both Managed Services and STMS Data Centre Services, regardless of Service Provider accounting treatment, is (the "**Service Provider Revenue**").

The costs associated with the Agreement and any BPS Services Agreement for both Managed Services and STMS Data Centre Services, regardless of Service Provider accounting treatment, is (the "**Service Provider Cost**"). The Service Provider Cost may include corporate allocations (for example, office space, computers used by Service Provider Personnel), where such allocation are related to the delivery of the Services under the Agreement and will be without duplication.

8.2 Annual Growth

The percentage by which the Fees have increased over the Baseline Fee plus Data Centre Fees collectively the Total Fees is (the "**Annual Growth**"). The Annual Growth is calculated as follows:

(Service Provider Revenue – Total Fees) / Total Fees.

The Baseline Fees (from Appendix C) plus the Data Centre Fees at the Effective Date are adjusted on an annual basis for inflation based on BC CPI. The Parties acknowledge that this is different from the inflation in Section 6.3 (*Managed Services Inflation*) and Section 6.4 (*STMS*

Data Centre Inflation), but have selected to apply only BC CPI to facilitate a less complex calculation.

The Baseline Fees will be pro-rated to match the Service Provider's fiscal year period. For example, the Service Provider's fiscal year is November 1 to October 31. Therefore, for the Margin Cap calculation at October 31, 2014, the Baseline Fees will be based on 5 months from Contract Year 13/14 and 7 months from Contract Year 14/15.

At issue for Inquiry

	Annual Growth	Margin Cap
Step 1	0% to up to 34%	24%
Step 2	34% to up to 66%	24% down to 23%
Step 3	66% to up to 100%	23% down to 22%
Step 4	At issue for Inquiry	

8.4 Profit Sharing Calculation

Based on the Annual Growth, the associated Margin Cap and the Service Provider Margin for the Service Provider's fiscal year, if the cumulative Service Provider Margin is greater than the Margin Cap percentage, then the Service Provider profit above that allowed at the Margin Cap percentage is shared by the Parties based on:

- 50% Service Provider; and
- 50% Province.

8.4.1 Timing of Margin Cap Calculation

At issue for Inquiry

If the Margin Cap was reached in the annual period for which the calculation is being performed, the Service Provider will credit the Province's share of the Margin Cap on the Province invoice following the calculation. The credit will not be an adjustment to the Unit Prices, but a credit given on the total invoice to the Province.

8.4.2 No Retro-Active Application of Margin Cap Sharing

At no time will prior year's revenues, which may or may not have involved a sharing of the Service Provider profit with the Province, be used in the current year's calculation except for the calculation of the cumulative Service Provider Margin.

Where there is a year of profit sharing followed by a year that has a cumulative Service Provider Margin below the Margin Cap percentage, the Province does not return any of the profit sharing from the prior year.

8.4.3 Example Margin Cap application

Refer to Appendix G for an example of how the Margin Cap is applied.

8.5 Financial Review of Margin Cap

8.5.1 Financial Monitor

The Province shall appoint a third party Financial Monitor who shall:

(a) validate the Service Provider Margin calculation as it relates to the Margin Cap, and to provide the Province an opinion that the Service Provider's calculation is correct, thereby determining if the Margin Cap as described in Section 8 (*Margin Cap*) has been reached; and

(b) confirm to the Province that the application of profit sharing above the Margin Cap has been treated correctly and in accordance with the provisions of this Section, where applicable.

The Province shall use reasonable efforts to engage the Financial Monitor on a long-term basis in order to provide the Province with the necessary information while minimizing the cost to Service Provider.

The Financial Monitor may not be a Competitor as listed in Schedule 5.

8.5.2 Financial Report

Service Provider shall provide the Financial Monitor with a financial summary of the Service Provider Revenue and Service Provider Cost, and calculated Service Provider Margin (the "**Financial Report**").

8.5.3 Service Provider Confidential Information

The Province acknowledges that the information contained in the Financial Report constitutes Service Provider Confidential Information. The Financial Report shall not be disclosed to any person except the Financial Monitor.

8.5.4 Access to the Financial Report

Service Provider shall provide access to the Service Provider Confidential Information (including the Financial Report) to the Financial Monitor and such employees thereof as require access to Service Provider Confidential Information in connection with the performance of their duties, and which employees have been approved by Service Provider acting reasonably, having

regard to the reputation of such individuals and their skills and experience in light of their job responsibilities (the "**Financial Monitor Team**").

Such individuals shall sign the Non-Disclosure Agreement at the time that the Financial Monitor Team is engaged.

8.5.5 Contract Roles for the Individuals with Access to the Financial Report

No individual who is a member of the Financial Monitor Team may be involved in the analysis of any Service Provider proposal to WTS during the period such individual is a member of the Financial Monitor Team and for a period of two years thereafter. If, as a result of a government reorganization, WTS is merged or combined with another Ministry, part or agency of the Government of British Columbia, then the above restriction relating to Service Provider proposals to WTS shall apply only to proposals submitted to the branch or division of the merged entity that is responsible for managing the Agreement, and shall not apply to the merged entity as a whole

If the Ministry hires any member of the Financial Monitor Team, then such individual shall not have any operational role in connection with the Agreement or provide any information or advice to the Ministry in conjunction with the Agreement or services provided by Service Provider to the Ministry for a period of two years after such individual is hired by the Ministry or such shorter period of time as is two years after the individual ceased to be a member of the Financial Monitor Team (the "**Restriction**"). If, as a result of a Government reorganization, the Ministry is merged or combined with another ministry, part or agency of the Government of British Columbia, then the Restriction shall apply only to the branch or division of the merged entity that is responsible for managing the Agreement and will not apply to the merged entity as a whole.

8.5.6 Frequency of Financial Reporting

The Financial Report, certified by the Service Provider CFO shall be provided by Service Provider to the Financial Monitor on an annual basis, when the Financial Monitor is engaged by the Province.

8.5.7 Audits of the Financial Reporting

The Financial Monitor may request further information from Service Provider in order to validate and confirm the accuracy of the Financial Report and such other information as may be required to validate the Service Provider Margin. The request for information may take the form of annual audits of the Service Provider financial system data. The following shall apply to the Financial Monitor:

(a) the Province shall cause all such audits to be performed during normal business hours and upon reasonable prior notice to Service Provider;

(b) the Province shall, and shall cause its representatives to:

(i) respect the scope and content of this Agreement in performing the audit of the Financial Report,

(ii) use reasonable efforts not to hinder or interfere with the performance of the Services by Service Provider, and for greater certainty, the Province acknowledges that to the extent any such exercise of rights directly hinders or interferes with Service Provider' ability to deliver the Services, then Service Provider shall not be responsible for any resulting Service Provider Service Level failures in respect thereof, and

(iii) comply with all security and other similar policies of Service Provider while at its premises, provided that Service Provider provides the Province with reasonable prior notice thereof;

(c) Service Provider shall be given the opportunity to respond to the audit results before they are finalized.

(d) The Financial Monitor will not have direct access to any Service Provider systems.

The Financial Monitor may request Service Provider data that would typically be part of an audit verification. Service Provider data requested by the Financial Monitor shall be provided by Service Provider on a timely basis. The audit is of Service Provider financial data related to the Agreement and does not allow the Financial Monitor access to financial data of Service Provider sub-contractors or data for other contracts. This section does not preclude the Financial Monitor from accessing sufficient Service Provider data to verify Service Provider' cost allocation processes.

8.5.8 Access to Detailed Audit Information

The Financial Monitor may not share the detailed or summary audit information with the Province. The Financial Monitor may provide an opinion to Service Provider and the Province as to the correctness of the Service Provider Margin calculation and application of the Margin Cap sharing.

The Province personnel with access to the opinion are:

(a) Deputy Minister, Ministry of Labour and Citizens' Services;

(b) ADM, Workplace Technology Services, Ministry of Labour and Citizens' Services;

(c) ADM, Executive Financial Officer of Ministry of Labour and Citizens' Services; and

(d) Executive Director, Enterprise Hosting Services (EHS), Ministry of Labour and Citizens' Services.

9. Refresh Schedule For Assets Used in the Provisioning of the Managed Services

Although Service Provider is responsible for determining the appropriate refresh schedule for Supported Infrastructure used in the provisioning of the Managed Services, it is anticipated that the refresh schedule for assets will be:

Equipment type	Estimate equipment life
Servers	At issue for Inquiry
Storage, backup and retention	
Mainframe	
Mainframe tape and DASD	
Network	

The parties acknowledge that from time to time an asset may be older than the equipment life in the table above, due to the planning and scheduling around the refresh cycle. The Parties agree that the life of an asset will not exceed the equipment life by more than 3 months.

S. 15

S. 15

At issue for Inquiry

9.1 Support of legacy Servers

A "**Legacy Server**" is a Server that exceeds At issue for Inquiry life, due to a restrictions or limitations of the application running on the Server, or some other requirement from the Province that prevent the Server from being refreshed. The Province has some Legacy Servers today, and other Servers may become Legacy Servers over the Term.

The following will apply to Legacy Servers:

(a) The SLA schedule addresses service levels for Legacy Servers.

(b) If the Legacy Server needs to be shipped to one of the STMS Data Centres, the Province is responsible for shipping costs.

(c) Service Provider will continue to support the Legacy Server at the then-current Midrange Services Unit Price so long as Service Provider's processes and tools are able support the Server.

(d) When support for the Legacy Server becomes more effort than Servers within their equipment life, Service Provider will inform the Province that the Legacy Server is unsupportable under the Managed Services Price Table rates (for example, the agents fail to report activity to the monitoring Servers, or the tools vendors no longer have software for the Legacy Server).

(e) Service Provider and the Province will agree, through the Change Order Process, that:

(i) the Province will make the required changes to the application or underlying reason why the Legacy Server cannot be refreshed, in order to make the refresh possible, or

(ii) a special Legacy Server support rate or a T&M support, whichever is most appropriate.

10. Termination Services Time and Material Rates

Appendix N – *Termination Services Time and Material Rates* sets forth a list of Standard Time and Materials Rates and Cost-Only Time and Materials Rates that apply to the Termination Services provided to the Province, which will be applied as described in Section 29.4 of the Agreement (*Charges for Terminations Services*).

The Province will treat the rates as Confidential and will only use and disclose the rates in accordance Section 16.7(b) (*Permitted Disclosure and Use of Confidential Information*) of the Agreement.

The Service Provider will calculate the Standard Time and Materials Rates and the Cost-Only Time and Materials Rates every two years taking into account inflation and changes in market conditions.

11. Definitions

"**000 GB Unit Price**" has the meaning given to it in Section 7.3.8.

"**Actual AES Hours**" has the meaning given to it in Section 5.5.

"**Actual Rebate**" has the meaning given to it in Section 5.6.2.

"**Additional Capacity Reservation**" means an increase to the Capacity Reservation of a BPS Customer in a given STMS Data Centre and may or may not increase the Province VA Commitment.

"**Adjusted Capacity Reservation**" means the sum of the Capacity Reservation of a BPS Customer in a given STMS Data Centre and any Additional Capacity Reservation of a BPS Customer in a given STMS Data Centre and may or may not increase the Province VA Commitment.

"**AES Hourly Overtime Rates**" has the meaning given to it in Section 5.4.3.

"**AES Hourly Rates**" has the meaning given to it in Section 5.4.2.

"**AES Minimum**" has the meaning given to it in Section 5.4.1.

"**AES Shortfall**" has the meaning given to it in Section 5.5.

"**Annual Growth**" has the meaning given to it in Section 8.2.

"**Base Unit Price**" has the meaning given to it in Section 3.1.4.

"**BCGEU Employees**" has the meaning given to it in Section 6.3.3.

"**BCGEU Inflation**" has the meaning given to it in Section 6.3.2.

"**BPS Customer**" has the meaning given to it in Section 4.5.

"**Cancellation Notice**" has the meaning given to it in Section 2.7.8.

"**Capacity Phase-in**" has the meaning given to it in Section 4.7.

"**Capacity Reservation**" means the total quantity of reserved VAs by a BPS Customer in a given STMS Data Centre and is a subset of the Province VA Commitment.

"**Capital Payment Estimate**" has the meaning given to it in Section 2.7.2.

"**Capital Payment Shortfall**" has the meaning given to it in Section 2.7.5.

"**Capital Payment Surplus**" has the meaning given to it in Section 2.7.5.

"**Capital Payment**" has the meaning given to it in Section 2.7.1.

"**Capital Purchases**" has the meaning given to it in Section 2.7.4.

"**Component**" has the meaning given to it in Section 6.3.3.

"**Data Centre Months**" has the meaning given to it in Section 4.7.

"**Early Availability Date**" has the meaning given to it in Section 4.4.

"**Early Capacity**" has the meaning given to it in Section 4.4.

"**Energy Report**" has the meaning given to it in Section 5.6.1.

"**Existing Data Centre Space**" has the meaning given to it in Section 4.12.

"**Expected Rebate**" has the meaning given to it in Section 5.6.2.

"**Final Inflation Calculation**" has the meaning given to it in Section 6.4.4.

"**Financial Monitor Team**" has the meaning given to it in Section 8.5.4.

"**Financial Report**" has the meaning given to it in Section 8.5.2.

"**First Inflation Estimate**" has the meaning given to it in Section 6.4.4.

"**Future Hardware Purchases**" has the meaning given to it in Section 2.7.6.

"**Hourly Rates**" has the meaning given to it in Section 5.8.

"**Individual Volume Band**" has the meaning given to it in Section 3.13.

"**Installation Date**" has the meaning given to it in Section 4.9.2.

"**kVA Unit Price**" has the meaning given to it in Section 4.14.

"**Legacy Servers**" has the meaning given to it in Section 9.1.

"**Managed Services Price Table**" has the meaning given to it in Section 2.1.

"**Margin Cap**" has the meaning given to it in Section 8.

"**Midrange SOWs**" has the meaning given to it in Section 2.2.

"**Milestone Payment**" has the meaning given to it in Section 5.1.

"**Net Rebate**" has the meaning given to it in Section 5.6.2.

"**New Data Centre Space**" has the meaning given to it in Section 4.12.

"**New Technology**" has the meaning given to it in Section 4.12.

"**Non-AES Work**" has the meaning given to it in Section 5.4.1.

"**Non-Capital Servers**" has the meaning given to it in Section 2.7.7.

"**Optional Midrange Services**" has the meaning given to it in Section 2.3.8.

"**Partial VA New Technology Transfer**" has the meaning given to it in Section 4.12.

"**Percentage Component Change**" has the meaning given to it in Section 6.3.3

"**Percentage Increase**" has the meaning given to it in Section 6.3.2.

"**Percentage Salary Change**" has the meaning given to it in Section 6.3.3.

"**Province Adjusted VA Commitment**" has the meaning given to it in Section 4.2.

"**Province Initial VA Commitment**" has the meaning given to it in Section 4.4.

"**Province Revised Initial VA Commitment**" has the meaning given to it in Section 4.6.

"**Province VA Commitment**" has the meaning given to it in Section 4.2.

"**Reconciliation Report**" has the meaning given to it in Section 3.4.

"**Retiring Platforms**" has the meaning given to it in Section 2.3.9.

"**Salary Baseline**" has the meaning given to it in Section 6.3.3.

"**Second Inflation Estimate**" has the meaning given to it in Section 6.4.4.

"**Service Provider Cost**" has the meaning given to it in Section 8.1.

"**Service Provider Margin**" has the meaning given to it in Section 8.1.

"**Service Provider Revenue**" has the meaning given to it in Section 8.1.

"**SFP Base Unit Price**" has the meaning given to it in Section 2.3.1.

"**SFP Incremental Unit Price**" has the meaning given to it in Section 2.3.1.

"**STMS Prices**" has the meaning given to it in Section 6.4.

"**Time Sheet System**" has the meaning given to it in Section 5.4.5.

"**Unit Price Increase**" has the meaning given to it in Section 4.12.

"**Unit Price**" has the meaning given to it in Section 2.1.

"**VA Discount**" has the meaning given to it in Section 4.13.1.

"**VA Fees**" has the meaning given to it in Section 4.1.

"**VA New Technology Transfer**" has the meaning given to it in Section 4.12.

"**VA Price Column**" has the meaning given to it in Section 4.6.

"**VA Price Row**" has the meaning given to it in Section 4.6.

"**VA Price Tables**" has the meaning given to it in Section 4.1.

"**VA Unit Price**" has the meaning given to it in Section 4.1.

"**Volume Band Adjustment**" has the meaning given to it in Section 3.1.4.

"**Volume Band Ranges**" has the meaning given to it in Section 3.1.2.

"**Volume Banding Table**" has the meaning given to it in Section 3.1.2.

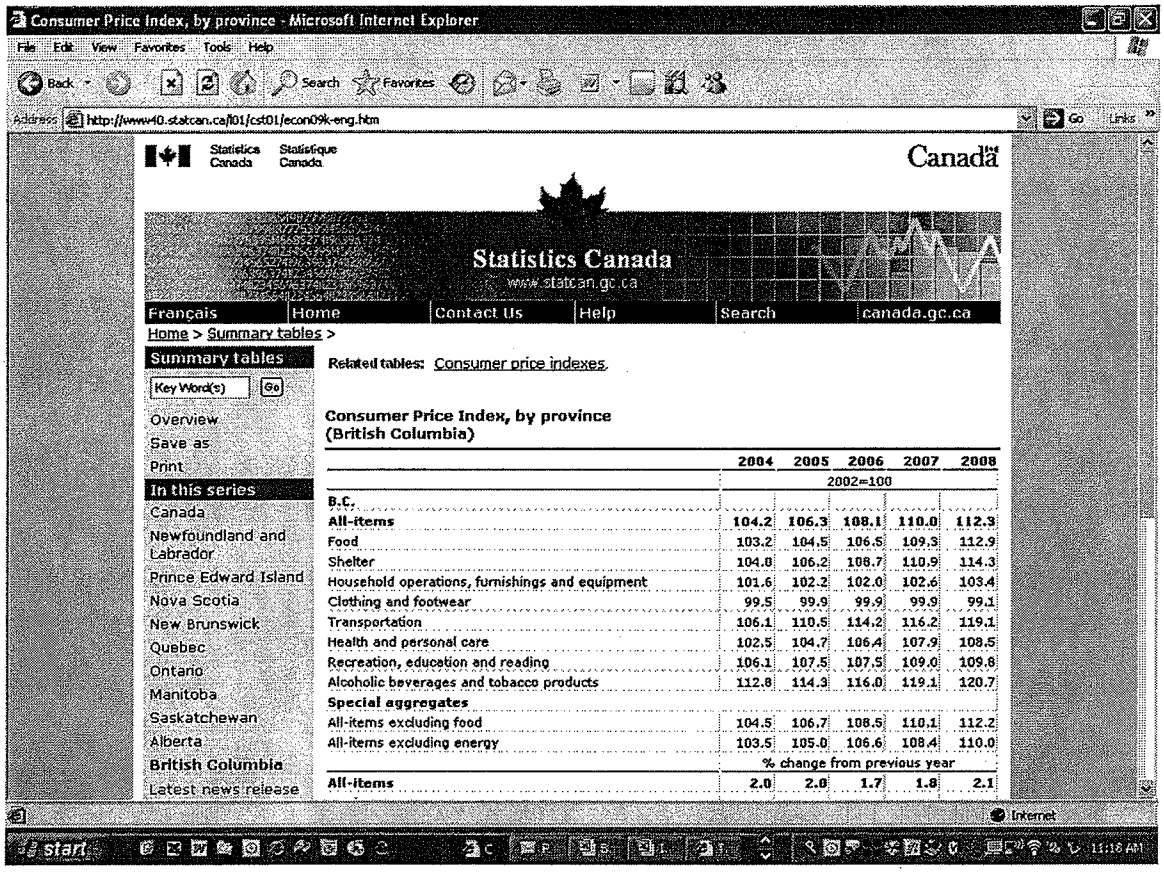
"**Volume Banding**" has the meaning given to it in Section 3.1.2.

Pages 1185 through 1335 redacted for the following reasons:
- -
At issue for Inquiry

SCHEDULE 23

APPENDIX E
BC CPI and DATA CENTRE CPI INSTRUCTIONS

DIAGRAM 1
Screen Shot of BC CPI website (current at February 2009)



Consumer Price Index, by province - Microsoft Internet Explorer

Statistics Canada — www.statcan.gc.ca

Français | Home | Contact Us | Help | Search | canada.gc.ca

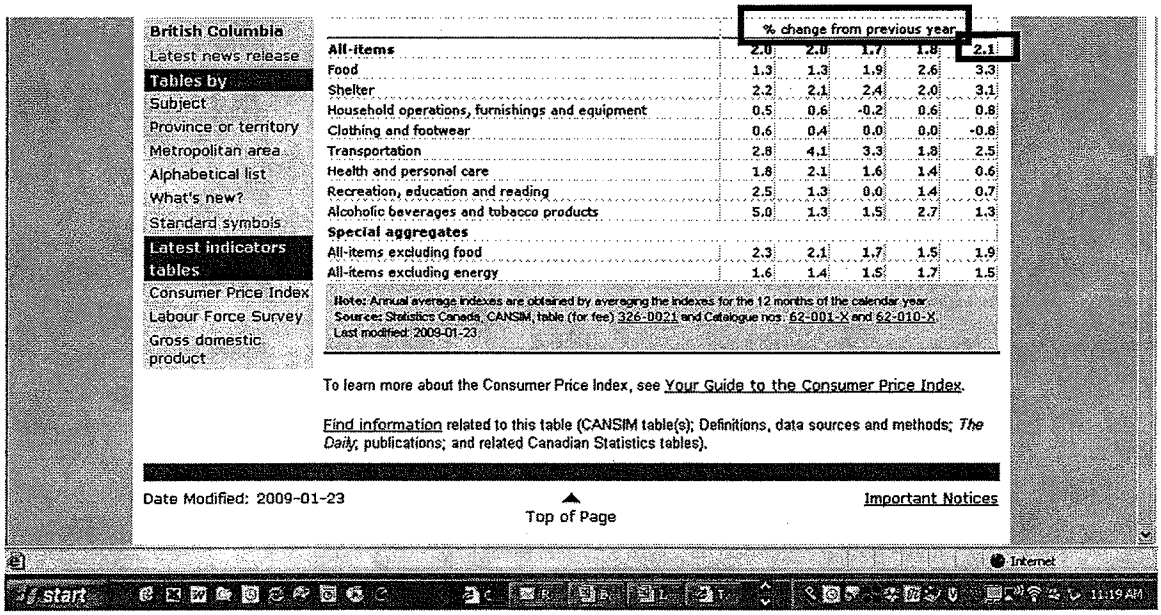
Home > Summary tables >

Summary tables

Related tables: Consumer price indexes.

Consumer Price Index, by province (British Columbia)

	2004	2005	2006	2007	2008
	2002=100				
B.C.					
All-items	104.2	106.3	108.1	110.0	112.3
Food	103.2	104.5	106.5	109.5	112.9
Shelter	104.0	106.2	108.7	110.9	114.3
Household operations, furnishings and equipment	101.6	102.2	102.0	102.6	103.4
Clothing and footwear	99.5	99.9	99.9	99.9	99.1
Transportation	106.1	110.5	114.2	116.2	119.1
Health and personal care	102.5	104.7	106.4	107.9	108.5
Recreation, education and reading	106.1	107.5	107.5	109.0	109.8
Alcoholic beverages and tobacco products	112.8	114.3	116.0	119.1	120.7
Special aggregates					
All-items excluding food	104.5	106.7	108.5	110.1	112.2
All-items excluding energy	103.5	105.0	106.6	108.4	110.0
	% change from previous year				
All-items	2.0	2.0	1.7	1.8	2.1



British Columbia | Latest news release | Tables by Subject | Province or territory | Metropolitan area | Alphabetical list | What's new? | Standard symbols | Latest indicators tables | Consumer Price Index | Labour Force Survey | Gross domestic product

	% change from previous year				
All-items	2.0	2.0	1.7	1.8	2.1
Food	1.3	1.3	1.9	2.6	3.3
Shelter	2.2	2.1	2.4	2.0	3.1
Household operations, furnishings and equipment	0.5	0.6	-0.2	0.6	0.8
Clothing and footwear	0.6	0.4	0.0	0.0	-0.8
Transportation	2.8	4.1	3.3	1.8	2.5
Health and personal care	1.8	2.1	1.6	1.4	0.6
Recreation, education and reading	2.5	1.3	0.0	1.4	0.7
Alcoholic beverages and tobacco products	5.0	1.3	1.5	2.7	1.3
Special aggregates					
All-items excluding food	2.3	2.1	1.7	1.5	1.9
All-items excluding energy	1.6	1.4	1.5	1.7	1.5

Note: Annual average indexes are obtained by averaging the indexes for the 12 months of the calendar year.
Source: Statistics Canada, CANSIM, table (for fee) 326-0021 and Catalogue nos. 62-001-X and 62-010-X.
Last modified: 2009-01-23

To learn more about the Consumer Price Index, see Your Guide to the Consumer Price Index.

Find information related to this table (CANSIM table(s); Definitions, data sources and methods; *The Daily*; publications; and related Canadian Statistics tables).

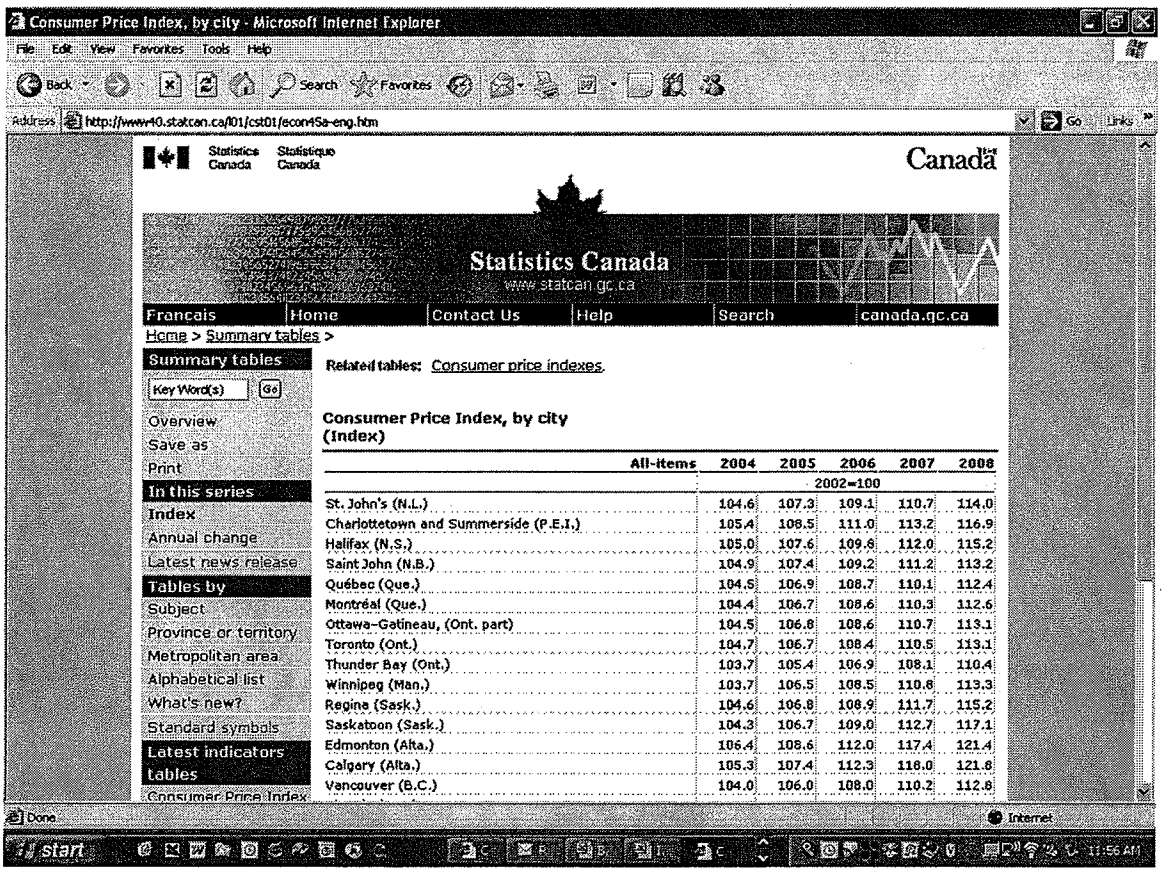
Date Modified: 2009-01-23 — Top of Page — Important Notices

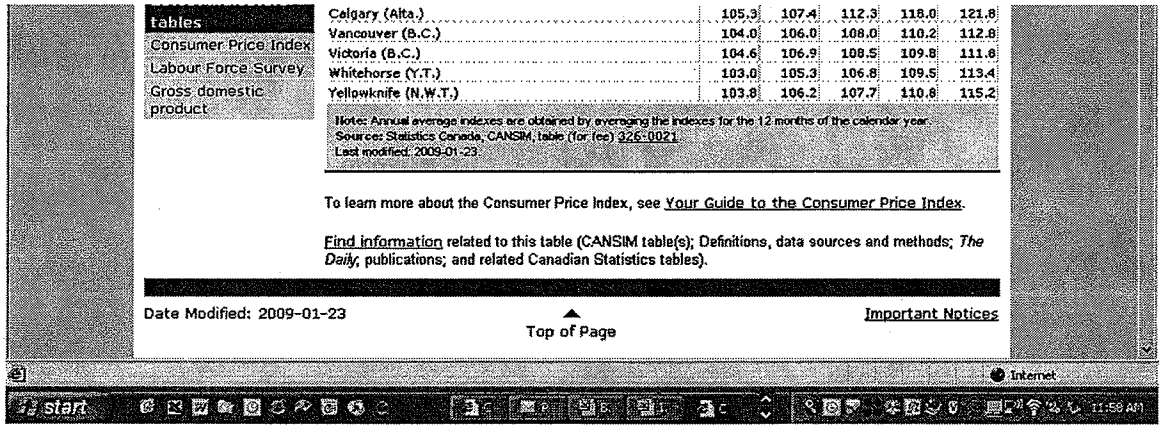
50652262.11

SCHEDULE 23

DIAGRAM 2

Screen shot of Data Centre CPI website (current as at February 2009)





SCHEDULE 23

CPI REPORT NUMBERS AND INSTRUCTIONS TO ACCESS THE CPI WEB SITES (CURRENT AS AT FEBRUARY 2009)

Statistics Canada, Consumer price index (CPI), 2005 basket, monthly (2002=100 unless otherwise noted) is Table 326-0020

- v41692924 Calgary, Alberta [48825]; All-items (2002=100) (monthly)
- v41692462 British Columbia; All-items (2002=100) (monthly)
- v41692930 Vancouver, British Columbia [59933]; All-items (2002=100) (monthly)

BC CPI can be access by:

- www.statcan.gc.ca
- Selecting "English"
- Select link on left-hand side of web site for "Summary Tables"
- Select link on left-hand side of web site under "Tables by" for "Province or Territory"
- Select link for "British Columbia"
- Select link for "Consumer Price Index, by province"
- The percentage inflation for BC CPI is the "% change from prior year"

Data Centre CPI can be access by:

- www.statcan.gc.ca
- Selecting "English"
- Select link on left-hand side of web site for "Summary Tables"
- Select link on left-hand side of web site under "Tables by" for "Metropolitan Area"
- Select link for "Vancouver (B.C.)" or "Calgary (Alta.)". Both links take the user to the same location.
- Select link for "Consumer Price Index, by city"
- Locate "Vancouver (B.C.)" and "Calgary (Alta.)" on the table.
- The percentage inflation for Data Centre CPI is the difference between the previous year and the year before the previous year, divided by 100. For example, at February 2009, the difference between 2008 and 2007 for Vancouver is (112.8-110.2)/100 = 0.026 or 2.6%.

Pages 1339 through 1397 redacted for the following reasons:
- -
At issue for Inquiry

SCHEDULE 23

APPENDIX J
SERVICES CATALOGUE

STMS Hosting Services

JSRFP No.: SATP - 231

SERVICE CATALOGUE
FISCAL YEAR 2009/2010

Author:	EDS Canada Inc.
Status:	FINAL
Release Date:	May 8, 2009
File Name:	Combined Service Catalogue

Statement of Confidentiality

This Service Catalogue is prepared in connection with the Due Diligence and Negotiation Phase of the Joint Solution Request for Proposal, JSRPF # SATP-231, for Strategic Transformation and Mainframe Services Project ("STMS Project"). This Service Catalogue contains confidential and proprietary information of the Her Majesty the Queen in Right of the Province of British Columbia, as represented by the Minister of Labour and Citizens' Services ("Ministry") and EDS Canada Inc. ("EDS"). This Service Catalogue is intended for use by the Ministry, and EDS for the STMS Project, and their respective authorized representatives. A separate Service Catalogue exists for use with broader public sector entities.

Table of Contents

General

This version of the Service Catalogue includes Unit Prices that are valid for the Province fiscal year 2009/2010.

The Unit Prices are those for the baseline volumes and the Service Catalogue does not address changes to the Unit Price(s) related to increases or decreases in volumes. Refer to Schedule 23, Volume Banding to understand how the Unit Prices change as volumes change.

The Unit Prices apply to the Province and an updated Service Catalogue will be created for use with Broader Public Sector entities.

Server Management Services

The Server Management Services provides for the deployment and daily delivery of Server hosting and management services to the Province (and Clients) consisting of procuring, installing, configuring, maintaining, upgrading, decommissioning and disposing of Servers and Server-related hardware, firmware, Operating Systems, backup and restore software, security software and monitoring software (such as anti-virus software, Server availability monitoring, patch management, Server performance monitoring), standard Server configuration, anti-virus, patch management and policy compliance. Server Management Services are available on a per month Unit Price and / or a one-time Unit Price basis. And the Unit Price is based on the Server size, Tier service level, type of operating system and function of the Server.

The Tier level of a Server indicates the Service Level that is applicable to the Server. Tier 1 indicates a clustered Server in a data centre with 7X24 support, Tier 2 indicates a single Server in a data centre and Tier 3 indicates a Server in a non-data centre location.

Production Servers:

- Application Server – Server that operates Applications in support of Province business processes. For example, Province owned/licensed and operated custom developed or COTS based Applications (such as MS Exchange, ERP applications, HealthNet, Citrix, Sharepoint);

- Database Server – Server that operates a Province Database Management System (DBMS) (such as Oracle, SQL Server);

- Web Hosting Server – Server that runs a web engine for a Province websites (such as Apache, Tomcat and IIS);

- Infrastructure Server – Server that does not require Applications, such as Active Directory, File Transfer Protocol (FTP) Servers. Infrastructure Servers do not run Province-facing applications, but run services that allow Province-facing and other applications to operate.

Development / Test Servers:

- Development / Test Server – Server that is used solely for developing and testing purposes and is not used for in the production environment. Any of the Servers referred to above may have an associated development/test Server.

Pages 1403 through 1416 redacted for the following reasons:
- -
At issue for Inquiry

Detailed Server Management Service Descriptions

Server Management Services	SKU #	Description	Specifications	Benefits
Tier 1 Windows Application, Database or Web Server	WAP-001	Windows Application, Database or Web Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Tier 1 Clusters are available in a data centre or as geo-clusters (across multiple data centres) • Data Centre based clusters target 99.95% availability • Asynchronous Geo-clusters target 99.99% availability • 7 x 24 support • Cluster Management • Requires two physical Servers (min) • Leverages EDS' Data Centre tools and availability • SAN connectivity as needed	highest level of availability. Intended for critical business applications
Tier 2 Windows Application, Database or Web Server	WAP-002	Windows Application, Database or Web Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12 or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on Virtual Servers • Virtual Server hosted in a VMware farm • Target for Virtual Servers to automatically recover upon host or image failure	Can be Physical Server(s) or Virtual

Server Management Services	SKU #	Description	Specifications	Benefits
Tier 3 Windows Application, Database or Web Server	WAP-003	Windows Application, Database or Web Server designed to have business priority level of availability and are not located in a Province or Service Provider Data Centre	Single hosting Server for the delivery of Business Priority service 5x8 or 7x24 support • Remote location	Dedicated server not located in a Province or Service Provider Data Centre
Tier 1 Windows Infrastructure Server	WIN-001	Windows Infrastructure Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Tier 1 Clusters are available in a data centre or as geo-clusters (across multiple data centres) • Data Centre based clusters target 99.95% availability • Asynchronous Geo-clusters target 99.99% availability • 7 x 24 support • Cluster Management • Requires two physical Servers (min) • Leverages EDS' Data Centre tools and availability • SAN connectivity as needed	highest level of availability. Intended for critical infrastructure
Tier 2 Windows Infrastructure Server	WIN-002	Windows Infrastructure Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12 or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on Virtual Servers • Virtual Server hosted in a VMware farm • Target for Virtual Servers to automatically recover upon host or	Can be Physical Server(s) or Virtual

Server Management Services	SKU #	Description	Specifications	Benefits
			image failure	
Tier 3 Windows Infrastructure Server	WIN-003	Windows Application, Database or Web Server designed to have business priority level of availability and are not located in a Province or Service Provider Data Centre	Single hosting Server for the delivery of Business Priority service 5x8 or 7x24 support • Remote location	Dedicated server not located in a Province or Service Provider Data Centre
Tier 1 Windows Development / Test Server	WDV-001	Windows Development / Test Servers are engineered to the same configuration as production Windows Tier 1 Servers, without Service Levels and reduced support	Clustered server (two or more nodes), engineered for delivering high levels of availability. Tier 1 Clusters are available in a data centre or as geo-clusters (across multiple data centres) • 7 x 24 support • Cluster Management • Requires two physical Servers (min) • Leverages EDS' Data Centre tools and availability • SAN connectivity as needed • Support effort is based on commercially reasonable expectations	Offers flexibility to configure, develop and test client applications as deemed necessary. It is not intended to host client production applications.

Server Management Services	SKU #	Description	Specifications	Benefits
Tier 2 Windows Development / Test Server	WDV-002	Windows Development / Test Servers are engineered to the same configuration as production Windows Tier 2 Servers, without Service Levels and reduced support	Single hosting server for the delivery of Business Priority service 5x9, 5x12 or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on Virtual Servers • Virtual Server hosted in a VMware farm • Target for Virtual Servers to automatically recover upon host or image failure	Offers flexibility to configure, develop and test client applications as deemed necessary. It is not intended to host client production applications. Can be physical server(s) or virtual
Tier 3 Windows Development / Test Server	WDV-003	Windows Development / Test Servers are engineered to the same configuration as production Windows Tier 2 Servers, without Service Levels and reduced support	Single hosting server for the delivery of Business Priority service 5x8 or 7x24 support • Server located external to Provincial or Service Provider Data Centre	Offers flexibility to configure, develop and test client applications as deemed necessary. It is not intended to host client production applications.
Tier 1 Solaris / Linux / AIX Application, Database or Web Server Support Services	UAP-001	Solaris / Linux / AIX Application, Database or Web Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Incorporates: • 7 x 24 support • Cluster Management • Requires two physical servers (min) • Data Centre Location only • SAN connectivity where necessary • Province to supply the required clustering software	Highest level of availability. Intended for critical business applications

Server Management Services	SKU #	Description	Specifications	Benefits
Tier 2 Solaris / Linux / AIX Application, Database or Web Server Support Services	UAP-002	Solaris / Linux / AIX Application, Database or Web Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12, or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on virtual servers	Can be physical server(s) or virtual
Tier 3 Solaris / Linux / AIX Application, Database or Web Server Support Services	UAP-003	Solaris / Linux / AIX Application, Database or Web Server designed to have business priority level of availability for non-Data Centre locations	Single hosting server for the delivery of Business Priority service 5x8 or 7x24 support • Server located external to Provincial or Service Provider Data Centre	Dedicated server in non-Data Centre location
Tier 1 Solaris / Linux / AIX Infrastructure Server Support Services	UIS-001	Solaris / Linux / AIX Infrastructure Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Incorporates: • 7 x 24 support • Cluster Management • Requires two physical servers (min) • Data Centre Location only • SAN connectivity where necessary • Province to supply the required clustering software	Highest level of availability. Intended for critical business applications
Tier 2 Solaris / Linux / AIX Infrastructure Server Support Services	UIS-002	Solaris / Linux / AIX Infrastructure Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12, or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on virtual servers	Can be physical server(s) or virtual
Tier 3 Solaris / Linux / AIX Infrastructure Server Support	UIS-003	Solaris / Linux / AIX Infrastructure Server designed to have business priority level	Single hosting server for the delivery of Business Priority service 5x8 or 7x24 support • Server located external to Provincial	Dedicated server in non-Data Centre location

Server Management Services	SKU #	Description	Specifications	Benefits
Services		of availability for non-Data Centre locations	or Service Provider Data Centre	
Tier 1 Solaris / Linux / AIX Development / Test Server	UDV-001	Solaris / Linux / AIX Development / Test Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Tier 1 Clusters are available in a data centre or as geo-clusters (across multiple data centres) • 7 x 24 support • Cluster Management • Requires two physical Servers (min) • Leverages EDS' Data Centre tools and availability • SAN connectivity as needed • Support effort is based on commercially reasonable expectations • Province to supply the required clustering software	Offers flexibility to configure, develop and test client applications as deemed necessary. It is not intended to host client production applications.
Tier 2 Solaris / Linux / AIX Development / Test Server	UDV-002	Solaris / Linux / AIX Development / Test Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12 or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on Virtual Servers • Virtual Server hosted in a VMware farm • Target for Virtual Servers to automatically recover upon host or image failure	Offers flexibility to configure, develop and test client applications as deemed necessary. It is not intended to host client production applications. Can be physical server(s) or virtual

Server Management Services	SKU #	Description	Specifications	Benefits
Tier 3 Solaris / Linux / AIX Development / Test Server	UDV-003	Solaris / Linux / AIX Development / Test Server designed to have business priority level of availability for non-Data Centre locations	Single hosting server for the delivery of Business Priority service 5x8 or 7x24 support • Server located external to Provincial or Service Provider Data Centre	Offers flexibility to configure, develop and test client applications as deemed necessary. It is not intended to host client production applications.
Tier 1 OpenVMS Application Server Support Services	OVAP-001	OpenVMS Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Incorporates: • 7 x 24 support • Cluster Management • Requires two physical servers (min) • Data Centre Location only • SAN connectivity where necessary	highest level of availability. Intended for critical business applications
Tier 2 OpenVMS Application Server Support Services	OVAP-002	OpenVMS Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12, or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on Virtual Servers	Can be Physical Server(s) or Virtual
Tier 3 OpenVMS Application Server Support Services	OVAP-003	OpenVMS Server designed to have business priority level of availability for non-Data Centre locations	Single hosting server for the delivery of Business Priority service 5x8 or 7x24 support • Server located external to Provincial or Service Provider Data Centre	Dedicated server in non-Data Centre location
Tier 1 OpenVMS Development / Test Server Support Services	OVDV-001	OpenVMS Server designed to have the highest level of availability	Clustered server (two or more nodes), engineered for delivering high levels of availability. Incorporates: • 7 x 24 support • Cluster Management • Requires two physical servers (min)	highest level of availability. Intended for critical business applications

Server Management Services	SKU #	Description	Specifications	Benefits
			• Data Centre Location only • SAN connectivity where necessary	
Tier 2 OpenVMS Development / Test Server Support Services	OVDV-002	OpenVMS Server designed to have business priority level of availability	Single hosting server for the delivery of Business Priority service 5x9, 5x12, or 7x24 support • Data Centre Location only • SAN connectivity where necessary • 3 month commitment on Virtual Servers	Can be Physical Server(s) or Virtual
Tier 3 OpenVMS Development / Test Server Support Services	OVDV-003	OpenVMS Server designed to have business priority level of availability for non-Data Centre locations	Single hosting server for the delivery of Business Priority service 5x8 or 7x24 support • Server located external to Provincial or Service Provider Data Centre	Dedicated server in non-Data Centre location

Detailed Infrastructure Descriptions

Note: All hardware server configurations below are based on a point in time, and will be continually updated with new specifications.

EDS Owned Server – Windows / Linux Server Hardware >$10K	SKU #	Description	Specifications
Server Hardware - Application >$10K	WLAPHW	Windows / Linux Application Server on EDS supplied hardware	Sun Fire X4240 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • x64 Capable • 2 AMD quad core processors • 8GB RAM • 2x146GB disks (Raid 1) • 2 Power Supplies
Server Hardware – Application Remote >$10K	WLAPHW-003	Windows / Linux Non Data Centre Application Server on EDS supplied hardware	Sun Fire X4240 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • x64 Capable • 2 AMD quad core processors • 8GB RAM • 2x146GB disks (Raid 1) 2 Power Supplies
Server Hardware - Development / Test > 10K	WLDVHW	Windows / Linux Development / Test Server on EDS supplied hardware	Sun Fire X4240 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • Redundant Multi-port SAN connections • x64 Capable • 2 AMD quad core processors • 8GB RAM • 2x146GB disks (Raid 1) • 2 Power Supplies 2x4GB HBAs

EDS Owned Server – Windows / Linux Server Hardware >$10K	SKU #	Description	Specifications
Server Hardware - Development / Test Remote > 10K	WLDVHW-003	Windows / Linux Non Data Centre Development / Test Server on EDS supplied hardware	Sun Fire X4240 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • Redundant Multi-port SAN connections • x64 Capable • 2 AMD quad core processors • 8GB RAM • 2x146GB disks (Raid 1) • 2 Power Supplies • 2x4GB HBAs
Server Hardware - Database > 10K	WLDBHW	Windows / Linux Database Server on EDS supplied hardware	Sun Fire X4240 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • Redundant Multi-port SAN connections • x64 Capable • 2 AMD quad core processors • 8GB RAM • 2x146GB disks (Raid 1) • 2 Power Supplies 2x4GB HBAs
Server Hardware - Web > 10K	WLWBHW	Windows/Linux Web Server on EDS supplied hardware	Sun Fire X4140 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • x64 Capable • 1 AMD quad core processor • 4GB Memory • 2x73GB disks (Raid 1) 2 Power Supplies

EDS Owned Server – Windows / Linux Server Hardware >$10K	SKU #	Description	Specifications
Server Hardware – Infrastructure >$10K	WLINHW	Windows/Linux Infrastructure Server on EDS supplied hardware	Sun Fire X4140 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • x64 Capable • 1 AMD quad core processor • 4GB Memory • 2x73GB disks (Raid 1) 2 Power Supplies
Server Hardware – Citrix >$10K	WLCXHW	Windows/Linux Citrix Server on EDS supplied hardware	Sun Fire X4140 server • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • x64 Capable • 1 AMD quad core processor • 4GB Memory • 2x73GB disks (Raid 1) • 2 Power Supplies

EDS Owned Server - Solaris / AIX / OpenVMS Hardware >$10K	SKU #	Description	Specifications
Server Hardware - Solaris - Application >$10K	SAPHW-S	Solaris Application Server on EDS supplied hardware	Sun SPARC T2000 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 4 core 1.2GHz UltraSparc T2 processor • 8GB Memory • 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs • 2 Power Supplies
Server Hardware - Solaris - Application >$10K	SAPHW-M	Solaris Application Server on EDS supplied hardware	Sun T5220 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 8 core 1.2GHz UltraSparc T2 processor • 32GB Memory • 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs • 2 Power Supplies

Server Hardware - Solaris - Application >$10K	SAPHW-L	Solaris Application Server on EDS supplied hardware	Sun SPARC Enterprise M4000 server • Optimized for 24x7 mission critical computing and large shared memory applications • Includes 4*2.4GHz SPARC64 VII four-core Processors (2 CPU boards with 2 *CPUS each & 5MB on-chip L2 cache) • 32GB system memory on (2 memory modules with 8 * 2GB DDR2 DIMMs) • 2 * 146GB SAS hard disks • 1 DVD-ROM • 2*Gb ethernet ports • 1 I/O tray with 4 PCI-E and 1 PCI-X slots • 2 power supplies (110V or 220V with N+N redundancy)
Server Hardware - Solaris – Development / Test >$10K	SDVHW-S	Solaris Development / Test Server on EDS supplied hardware	Sun SPARC T2000 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 4 core 1.2GHz UltraSparc T2 processor • 8GB Memory • 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs • 2 Power Supplies
Server Hardware - Solaris – Development / Test >$10K	SDVHW-M	Solaris Development / Test Server on EDS supplied hardware	Sun T5220 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 8 core 1.2GHz UltraSparc T2 processor • 32GB Memory

			• 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs 2 Power Supplies
Server Hardware - Solaris – Development / Test >$10K	SDVHW-L	Solaris Development / Test Server on EDS supplied hardware	Sun SPARC Enterprise M4000 server • Optimized for 24x7 mission critical computing and large shared memory applications • Includes 4*2.4GHz SPARC64 VII four-core Processors (2 CPU boards with 2 *CPUS each & 5MB on-chip L2 cache) • 32GB system memory on (2 memory modules with 8 * 2GB DDR2 DIMMs) • 2 * 146GB SAS hard disks • 1 DVD-ROM • 2*Gb ethernet ports • 1 I/O tray with 4 PCI-E and 1 PCI-X slots • 2 power supplies (110V or 220V with N+N redundancy)
Server Hardware - Solaris - Database >$10K	SDBHW-S	Solaris Database Server on EDS supplied hardware	Sun SPARC T2000 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 4 core 1.2GHz UltraSparc T2 processor • 8GB Memory • 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs • 2 Power Supplies •

Server Hardware - Solaris - Database >$10K	SDBHW-M	Solaris Database Server on EDS supplied hardware	Sun T5220 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 8 core 1.2GHz UltraSparc T2 processor • 32GB Memory • 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs • 2 Power Supplies
Server Hardware - Solaris - Database >$10K	SDBHW-L	Solaris Database Server on EDS supplied hardware	Sun SPARC Enterprise M4000 server • Optimized for 24x7 mission critical computing and large shared memory applications • Includes 4*2.4GHz SPARC64 VII four-core Processors (2 CPU boards with 2 *CPUS each & 5MB on-chip L2 cache) • 32GB system memory on (2 memory modules with 8 * 2GB DDR2 DIMMs) • 2 * 146GB SAS hard disks • 1 DVD-ROM • 2*Gb ethernet ports • 1 I/O tray with 4 PCI-E and 1 PCI-X slots • 2 power supplies (110V or 220V with N+N redundancy) •
Server Hardware - Solaris - Web >$10K	SWBHW-S	Solaris Web Server on EDS supplied hardware	Sun SPARC T2000 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 4 core 1.2GHz UltraSparc T2 processor • 8GB Memory • 3x146GB disks (Raid 1, hot

			spare) • 2 Dual Port 4Gb HBAs 2 Power Supplies
Server Hardware - Solaris - Web >$10K	SWBHW-M	Solaris Web Server on EDS supplied hardware	Sun T5220 server • Enterprise Class Server • Coolthreads technology (extremely power efficient while maintaining high throughput) • Highly available server with redundant internal storage and power supplies • Multiple network connections dedicated for user data traffic • 8 core 1.2GHz UltraSparc T2 processor • 32GB Memory • 3x146GB disks (Raid 1, hot spare) • 2 Dual Port 4Gb HBAs 2 Power Supplies
Server Hardware - Solaris - Web >$10K	SWBHW-L	Solaris Web Server on EDS supplied hardware	Sun SPARC Enterprise M4000 server • Optimized for 24x7 mission critical computing and large shared memory applications • Includes 4*2.4GHz SPARC64 VII four-core Processors (2 CPU boards with 2 *CPUS each & 5MB on-chip L2 cache) • 32GB system memory on (2 memory modules with 8 * 2GB DDR2 DIMMs) • 2 * 146GB SAS hard disks • 1 DVD-ROM • 2*Gb ethernet ports • 1 I/O tray with 4 PCI-E and 1 PCI-X slots • 2 power supplies (110V or 220V with N+N redundancy)
Server Hardware - AIX – Application >$10K	AAPHWM	AIX Application, Server on EDS supplied hardware	IBM System p550 • six 146 GB 15k hard drives • 32 GB RDIMMs 667 MHz 512Mb DRAM • 6 dual-core 3.5 GHz POWER6 Processors (4 activated) • 2 Dual port HBA • 4 dual port GB PCI-X NIC

Server Hardware - AIX – Database >$10K	ADBHW-M	AIX Database Server on EDS supplied hardware	IBM System p550 • six 146 GB 15k hard drives • 32 GB RDIMMs 667 MHz 512Mb DRAM • 6 dual-core 3.5 GHz POWER6 Processors (4 activated) • 2 Dual port HBA 4 dual port GB PCI-X NIC
Server Hardware - AIX – Development / Test >$10K	ADVHW-M	AIX Development / Test Server on EDS supplied hardware	IBM System p550 • six 146 GB 15k hard drives • 32 GB RDIMMs 667 MHz 512Mb DRAM • 6 dual-core 3.5 GHz POWER6 Processors (4 activated) • 2 Dual port HBA 4 dual port GB PCI-X NIC
Server Hardware - OpenVMS – Application >$10K	OVAPHW	OpenVMS Application Server on EDS supplied hardware	HP rx3600 • 2x1.42GHz/12MB 9120N • 8GB DDR2 (2x1GB) Memory • 2 x HP Integrity 36GB 15k SAS Drive • HP Integrity DVD-ROM Drive • 2 x HP PCI-X 2.0 1Port 4Gb Fibre Channel HBA • 2 x HP Integrity Redundant Power Supply • HP Integrity Upgraded Core I/O with VGA
Server Hardware - OpenVMS – Development / Test >$10K	OVDVHW	OpenVMS Development / Test Server on EDS supplied hardware	HP rx3600 • 2x1.42GHz/12MB 9120N • 8GB DDR2 (2x1GB) Memory • 2 x HP Integrity 36GB 15k SAS Drive • HP Integrity DVD-ROM Drive • 2 x HP PCI-X 2.0 1Port 4Gb Fibre Channel HBA • 2 x HP Integrity Redundant Power Supply • HP Integrity Upgraded Core I/O with VGA

EDS Owned Server – Software & SW Maintenance – Windows / Linux	SKU #	Description	Specifications
Server Software & Software Maintenance – Application	WLAPSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath - Antivirus
Server Software & Software Maintenance – Development / Test	WLDVSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath - Antivirus
Server Software & Software Maintenance – Database	WLDBSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath - Antivirus
Server Software & Software Maintenance – Web	WLWBSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath - Antivirus
Server Software & Software Maintenance – Infrastructure	WLINSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath - Antivirus
Server Software & Software Maintenance – Citrix	WLCXSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath - Antivirus

EDS Owned Server – Software & SW Maintenance – Solaris/ AIX / OpenVMS	SKU #	Description	Specifications
Server Software & Software Maintenance – Solaris – Application >$10K	SAPSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – Solaris - Development / Test >$10K	SDVSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – Solaris Database >$10K	SDBSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – Solaris Web >$10K	SWBSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – AIX Application >$10K	AAPSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – AIX Database >$10K	ADBSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath

EDS Owned Server – Software & SW Maintenance – Solaris/ AIX / OpenVMS	SKU #	Description	Specifications
Server Software & Software Maintenance – AIX Development / Test >$10K	ADVSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – OpenVMS – Application >$10K	OVAPSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath
Server Software & Software Maintenance – OpenVMS – Development / Test >$10K	OVDVSW	Monthly rate for the Service Provider provided software per Server	Server Provided software such as; - EMC PowerPath

Virtual Server Windows Services		Description
Windows Guest Application Virtual Server	VWGAP	Windows Virtual Application Server for Tier 1 or Tier 2 Services
Windows Guest Web Virtual Server	VWGWB	Windows Virtual Web Server for Tier 1 or Tier 2 Services
Windows Guest Database Virtual Server	VWGDB	Windows Virtual Database Server for Tier 1 or Tier 2 Services
Windows Guest Infrastructure Virtual Server	VWGIN	Windows Virtual Database Server for Tier 1 or Tier 2 Services
Windows Guest Development / Test Virtual Server	VWGDV	Windows Virtual Database Server for Tier 1 or Tier 2 Services

Virtual Server LINUX Services	Description	
Linux Guest Application Virtual Server	VLGAP	Linux Virtual Application Server for Tier 1 or Tier 2 Services
Linux Guest Web Virtual Server	VLGWB	Linux Virtual Web Server for Tier 1 or Tier 2 Services
Linux Guest Database Virtual Server	VLGDB	Linux Virtual Database Server for Tier 1 or Tier 2 Services
Linux Guest Infrastructure Virtual Server	VLGIN	Linux Virtual Infrastructure Server for Tier 1 or Tier 2 Services
Linux Guest Development / Test Virtual Server	VLGDV	Linux Virtual Infrastructure Server for Tier 1 or Tier 2 Services

Solaris Container & AIX WPAR Virtual Server Services		Description
Solaris Container Application Virtual Server	SCAP	Solaris Virtual Application Server for Tier 1 or Tier 2 Services
Solaris Container Web Virtual Server	SCAP	Solaris Virtual Web Server for Tier 1 or Tier 2 Services
Solaris Container Database Virtual Server	SCDB	Solaris Virtual Database Server for Tier 1 or Tier 2 Services
Solaris Container Development / Test Virtual Server	SCDV	Solaris Virtual Development / Test Server for Tier 1 or Tier 2 Services
AIX WPAR Application Virtual Server	AWAP	AIX Virtual Application Server for Tier 1 or Tier 2 Services
AIX WPAR Database Virtual Server	AWDB	AIX Virtual Database Server for Tier 1 or Tier 2 Services

AIX WPAR Development / Test Virtual Server	AWDV	AIX Virtual Development / Test Server for Tier 1 or Tier 2 Services

PORTION OF HOST SERVER HARDWARE EDS OWNED >$10K	SKU #	Description
Windows / Linux Host Server Hardware Support	VWLHS	Portion of a Physical Host Server for the support and delivery of a virtual server
Solaris Host Server Hardware Support	VSHS	Portion of a Physical Host Server for the support and delivery of a virtual server
AIX Host Server Hardware Support	VAHS	Portion of a Physical Host Server for the support and delivery of a virtual server

INITIAL INSTALL	SKU #	Description	Specifications
Windows or Linux (physical Server or Host Server) Install	WIN-LIN-INST	Services necessary for the implementation of a physical Windows or Linux Server	Perform the following tasks such as; - Assign a Server Name - Assign a IP address - Perform security scan - Perform compliance scan - Install the Server into a Server rack - Plug in the server to the appropriate network ports and power feeds - Provide the Client access to the Server
Solaris/AIX (physical Server or Host Server) Install	SOL-AIX-INST	Services necessary for the implementation of a physical Solaris or AIX Server	Perform the following tasks such as; - Assign a Server Name - Assign a IP address - Perform security scan - Perform compliance scan - Install the Server into a Server rack - Plug in the server to the appropriate network ports and power feeds Provide the Client access to the Server
Open VMS (physical Server; N/A Host Server) Install	OVMS-INST	Services necessary for the implementation of a physical OpenVMS Server	Perform the following tasks such as; - Assign a Server Name - Assign a IP address - Perform security scan - Perform compliance scan - Install the Server into a Server rack - Plug in the server to the appropriate network ports and power feeds Provide the Client access to the Server
VMware (Physical Host Server) Install	VM-INST	Services necessary for the implementation of a physical VMware Server	Perform the following tasks such as; - Assign a Server Name - Assign a IP address - Perform security scan - Perform compliance scan - Install the Server into a Server rack - Plug in the server to the appropriate network ports

			and power feeds Provide the Client access to the Server
Solaris / AIX (Virtual Server) Install	SOLV-AIXV-INST	Services necessary for the implementation of a virtual Solaris or AIX Server	Perform the following tasks such as; - Assign a Server Name - Assign a IP address - Perform security scan - Perform compliance scan Provide the Client access to the Server

Detailed Mid-Range Optional Service Descriptions

OTHER MID-RANGE SERVICES	SKU #	Description	Specifications	Benefits
Citrix Server Support	CTX-100	An uplift charge for the installation and operation of Citrix services, a necessary charge for establishing a Citrix server.	Install Citrix to the farms current level (i.e. Version 4.5) integrate into Province farm	Allows application publishing

MIDDLE-WARE SUPPORT	SKU #	Description	Specifications	Benefits
Apache	APA-100	An uplift service for the installation, operation and support of a dedicated Apache web server on a Client Application Server.	Includes a supported version of Apache on Linux.	Provides management services for web services support
Tomcat	TOM-100	An uplift service for the installation, operation and support of a dedicated Tomcat web server on a Client Application Server	Includes a supported version of Apache on Linux.	Provides management services for web services support
IIS (Internet Information Server)	IIS-100	An uplift service for the installation, operation and support of a dedicated IIS web server on a Client Application Server	Includes a supported version of IIS on a support version of Windows.	Provides management services for web services support

WINDOWS / LINUX SERVER OPTIONAL SERVICES	SKU #	Description	Specifications	Benefits
Application monitoring services	WLAM-100	Service for adding application monitoring to a server	EDS Standard monitoring agent set to monitor client specified measures and thresholds. Provides notifications to Clients based on configuration.	Leverages the Service Provider's monitoring infrastructure and support
Batch scheduling service	WLBS-100	Services for adding batch scheduling to a server	Work with the Client to determine their Batch scheduling needs and add the resultant schedule to EDS' standard batch monitoring tool	Leverages the Service Provider's monitoring infrastructure and support
Batch management services	WLBM-100	Service for adding batch job monitoring for a server	EDS Standard batch monitoring agent established for the monitoring of application batch schedules notifications	Leverages the Service Provider's monitoring infrastructure and support
Database management services	WLDB-100	Service for the installation and operation of Relational Database Management Software,	System DBA support for Oracle or SQL Server	Optional database support
Cluster management	WLCM-100	Service for the installation and management of Cluster software on a server	Cluster management software operation and support	Solution can be applied to Tier 2, Tier 3 servers.
Image performance management	WLPM-100	Service for adding image performance	EDS Standard monitoring agent set to	Enhanced reporting and monitoring service.

WINDOWS / LINUX SERVER OPTIONAL SERVICES	SKU #	Description	Specifications	Benefits
		management software and support to a server	monitor the performance of Client applications. Thresholds and measures are specified by the Client and the services provides enhanced reporting capabilities.	Client defined thresholds and reporting.
Server Capacity planning	WLCP-100	Service for adding capacity management software and support to a server	EDS Standard monitoring software monitors server capacity and provides trending reports on resources including CPU, memory, and disk usage.	Enhanced understanding of capacity requirements and enables projections of future requirements. Identifies potential performance challenges in a preventive fashion
Disaster Recovery Plan/Test	WLDR-100	Service for adding Disaster Recovery Planning and Testing to a server. Cost for this service is quotable per engagement.	As to be determined by the Client this service can define, test and maintain Clients' Disaster Recovery Plan documents for hosting related elements (hardware, IP addressing, server name, O/S, etc)	Scales to Client needs.
Extended Support Hour - 5 x 12	WL5x12-100	Service for increasing server management hours from 5 x 9 to 5 x 12	Pager support for additional hours 7AM – 7PM	Extended hours of support
Extended Support Hour - 7 x 24	WL7x24-100	Service for increasing server management hours from 5 x 9	Pager support for additional hours.	Extended hours of support

WINDOWS / LINUX SERVER OPTIONAL SERVICES	SKU #	Description	Specifications	Benefits
		to 7 x 24		
Extended Support Hour Uplift - remote field services - 7 x24	WL7x24R-100	Service for increasing remote (i.e. Non-data centre locations) server management hours from 5 x 9 to 7 x 24	Pager support for additional hours. Field support for additional hours.	Extended hours of support

SOLARIS / AIX OPTIONAL SERVICES	SKU #	Description	Specifications	Benefits
Application monitoring services	SAAM-100	Service for adding application monitoring to a server or servers	EDS Standard monitoring agent set to monitor client specified measures and thresholds. Provides notifications to Clients based on configuration.	
Batch monitoring services	SABM-100	Service for adding batch job monitoring to a server	Work with the Client to determine their Batch scheduling needs and add the resultant schedule to EDS' standard batch monitoring tool	
Batch scheduling services	SABS-100	Services for adding batch scheduling to a server	EDS Standard batch monitoring agent established for the monitoring of application batch schedules notifications	
Database Management Services	SADB-100	Service for the installation and operation of Database software services, a necessary charge for establishing an database server	System DBA support for Oracle or SQL Server	
Cluster Management	SACM-100	Service for adding Cluster Management to a server or servers	Cluster management software operation and support	

SOLARIS / AIX OPTIONAL SERVICES	SKU #	Description	Specifications	Benefits
Image Performance Management	SAPM-100	An uplift Service for adding Performance Management and Reporting to a server or servers	EDS Standard monitoring agent set to monitor the performance of Client applications. Thresholds and measures are specified by the Client and the services provides enhanced reporting capabilities.	
Server Capacity Planning	SACP-100	An uplift Service for adding Capacity Planning & Reporting to a server or servers	EDS Standard monitoring software monitors server capacity and provides trending reports on resources including CPU, memory, and disk usage.	
DR Recovery Plan/Test	SADR-100	An uplift Service for adding DR Recovery Planning and Testing to a server or servers	As to be determined by the Client this service can define, test and maintain Clients' Disaster Recovery Plan documents for hosting related elements (hardware, IP addressing, server name, O/S, etc)	
Extended Support Hour - 5 x 12	SA5x12-100	Service for increasing server management hours from 5 x 8 to 5 x 12	Pager support for additional hours 7AM – 7PM	

SOLARIS / AIX OPTIONAL SERVICES	SKU #	Description	Specifications	Benefits
Extended Support Hour - 7 x 24	SA7x24-100	Service for increasing server management hours from 5 x 8 to 7 x 24	Pager support for additional hours.	
Extended Support Hour - remote field - 7 x24	SA7x24R-100	Service for increasing remote (i.e. Non-data centre locations) server management hours from 5 x 8 to 7 x 24	Pager support for additional hours. Field support for additional hours.	

Detailed Mid-Range Shared Service Descriptions

SHARED SERVICE	SKU #	Description	Specifications	Benefits
Shared File and Print Service – Base Unit	SFP-001	A cross-government file and print queue hosting service	***FILE SERVICES*** • Client access to shared network folders for storing data files • Definition, support, and maintenance of file access control standards, including file and folder security to a maximum of three levels • Basic reporting and management tools for file services are available to Client LAN Administrators ***PRINT SERVICES*** • Access to shared network printers for printing user data files • Definition, support and maintenance of print queue access control standards • Basic reporting and management tools for print services to Client LAN Administrators ***SERVER STORAGE***	

SHARED SERVICE	SKU #	Description	Specifications	Benefits

			• A base allocation of server storage to a Client organization for the use of home drives and group shares
			• The Client organization's total base allocation is calculated using the number of SFP users multiplied by 1.5 gigabytes (GB)
			• Additional incremental storage over the client organization's total base allocation is available
			DATA BACKUP AND RESTORE SERVICES
			• Daily backups of user data files and folders are made in order to minimize data loss in the event of a system outage or accidental deletion.
			• File retention
			  • Sixty-day retention on all files existing more than one day
			  • Two-year retention on all files existing more than one month
			  • For individual files requiring longer retention, please see the Data Backup	

SHARED SERVICE	SKU #	Description	Specifications	Benefits
			Service • Restore Services • File restores can be performed upon request, when necessary. ***INFRASTRUCTURE MANAGEMENT AND SUPPORT*** • Installation and management of server hardware and software • System level testing of new printer drivers on SFP servers, and maintenance of an "Approved SFP Printers" list • Configuration and management of print queue and software driver installation on SFP servers	
Shared File and Print Queue Service		A cross-government print queue hosting service	Access to shared network printers for printing user data files Definition, support and maintenance of print queue access control standards Basic reporting and management tools for print services to client LAN Administrators Print queue management for Workstation Services clients (see Related Services)	

SHARED SERVICE	SKU #	Description	Specifications	Benefits
Dedicated SFP Server	DSFP-001	A dedicated Shared File/Print server to a single client	Dedicated SFP servers can be placed at the Client's site to meet business requirements. This is a quotable service and will be priced on a case-by-case basis.	
Shared File and Print Services Incremental 1.0GB	ISSFP-100	A charge for use for storage consumption beyond 1.5 gigabytes (GB) / User	Consumption is measured on a aggregate basis for each Client organization. Incremental storage fees are for storage exceeding the Client organizations SFP allocation. Service includes storage management services and backup restore services.	
Shared Database Services	SDBS-001	A cross-government optional shared database hosting service	One instance of a database, management environment and standard backup for each instance. Instances can be used for any environment such as production, test or development. Maintenance of a database environment that supports applications developed using ODBC and a wide variety of tools (Visual BASIC, C, Oracle Forms, Java, Visual Interdev, Excel, SQL*Net) An evaluation of requirements and technology to determine whether the Shared Database Service meets the needs of the application Agreement based on the required disk space, backup and service requirements Enabling of the desktop application through reconfiguration, modification or re-writing with a compliant development tool.	

SHARED SERVICE	SKU #	Description	Specifications	Benefits
			Creation of the database environment (additional hardware, data store, database objects, management directories, and data backup/restore procedures). Clients are required to purchase an additional shared database (test or development) to go along with the production database at the same cost as the production database. If a client does not have a test or dev database on the Shared Database Service, their production database will be considered a test database.	
Shared Database Services - Incremental 1.0 GB	ISDBS-100	A charge for use for storage consumption beyond 5 GB / Database	Consumption is measured per database, and incremental storage fees are calculated for storage usage exceeding the 5GB per database allocation. Service includes storage management services and backup restore services.	
Shared Web Hosting Services	SWHS-001	A cross-government web server hosting service	This service is for IIS web services and includes the creation of one website (top level folder) with a unique IP address and a domain name within the government namespace. Service also includes website configuration, FTP site, single network share, FrontPage extensions, indexing service catalogue, and initial file system security configuration that allows Clients full control over	

SHARED SERVICE	SKU #	Description	Specifications	Benefits
			content. Dynamic websites require a test or development shared web hosting site in addition to the dynamic production site..	
Shared Web Services – Incremental 0.5 GB	ISSWHS-001	A charge for use for storage consumption beyond 500 MB allocation per website	Consumption is measured per website, and incremental storage fees are calculated for storage usage exceeding the 500MB per website allocation. Service includes storage management services and backup restore services.	

Managed Storage & Managed Backup Services

Managed Storage Services

Managed Storage Services is the management of the storage of Data in storage tiers (Tier 1, 2, 3) based upon performance and reliability required for such Data. The storage tiers are distinguished by the performance of the disk and the Storage Array (the amount of cache memory, speed and size of the disk and the size of the RAID group) and the reliability of the disk and the Storage Array (the type of Storage Array with its underlying redundancy components and the size of the RAID group). The Managed Storage Services establish the data storage foundation required to support the Province Data storage requirements. The Service Provider will use integrated Storage Hardware, Storage Software, and support solutions to provide the Managed Storage Services within the range of data storage tiers identified, as appropriate. All storage volumes are priced in allocated gigabytes.

Managed Backup Services

Managed Backup Services is the management of the Backup and restoration of data structured to meet requirements of accessibility, integrity, and recoverability (for example, basic tape-based Backup to disk-based Backup (VTL)). The Service Provider will use integrated Backup Hardware, Backup Software, and services to protect the Data.

Pages 1457 through 1463 redacted for the following reasons:
- -
At issue for Inquiry

Managed Storage Service Descriptions

Storage Service	SKU #	Description	Specifications	Benefits
Managed Storage Management Services Tier 1	SAN-001	Managed Tier 1 Storage is designed for increased scalability and performance over the other SAN tiers. The package enables additional value by allowing volume adjustments, reallocation, or reconfiguration as needed supporting growth provisioning within 24 hours. Application profiles for this service include simple business applications, databases, and static presentation layer requirements.	• Highly scalable enterprise storage platform • RAID 5 • Monitoring, configuration, control, and tuning software • Storage solution design with reliability, manageability, and scalability • Increased ability to dynamically increase key service attributes (options) • Continuous operational support (24x7x365) • Volume adjustments, reallocation, or reconfiguration as needed supporting growth	• A storage foundation able to take advantage of Information Lifecycle management • Reduced provisioning time to meet business demands • World-class managed services that satisfy your unique requirements • Consistent delivery, cost efficiency, operations service excellence, and peak technological innovation

Storage Service	SKU #	Description	Specifications	Benefits
			provisioning within 24 hour • Information availability of 99.999 percent • Client multi-path services • Inherent technology refresh services	
Managed Storage Management Services Tier 2	SAN-002	Managed Tier 2 SAN Storage brings scalability, reliability, and performance in an economical entry point into a sophisticated SAN. This service targets your midrange environment, offering availability to support non-critical data. Tier 2 addresses business needs with mid-level performance and a cost-effective solution	• RAID 5 • Monitoring, configuration, control, and tuning software • Storage solution design with reliability, manageability, and scalability • Increased ability to dynamically increase key service attributes (options) • Continuous operational support (24x7x365) • Volume adjustments, reallocation, or reconfiguration as needed	• A storage foundation able to take advantage of Information Lifecycle management • Utility reduces provisioning time to meet business demands • World-class managed services that satisfy your unique requirements • Consistent delivery, cost efficiency, operations service excellence, and peak technological innovation

Storage Service	SKU #	Description	Specifications	Benefits
			supporting growth provisioning within 24 hours • Information availability of 99.99 percent • Client multi-path services • Inherent technology refresh services	
Managed Storage Management Services Tier 3	SAN-003	Tier 3 SAN Storage brings scalability, reliability, and performance in an economical entry point into a sophisticated SAN. This service targets your midrange environment, offering availability to support non-critical data. Tier 3 Addresses your business needs with basic performance and a very cost-effective solution	• RAID 5 • Monitoring, configuration, control, and tuning software • Storage solution design with reliability, manageability, and scalability • Increased ability to dynamically increase key service attributes (options) • Continuous operational support (24x7x365) • Volume adjustments, reallocation, or reconfiguration as needed supporting growth	• A storage foundation able to take advantage of Information Lifecycle management • Utility reduces provisioning time to meet business demands • World-class managed services that satisfy your unique requirements • Consistent delivery, cost efficiency, operations service excellence, and peak technological innovation

Storage Service	SKU #	Description	Specifications	Benefits
			provisioning within 24 hours • Information availability of 99.9 percent (if using client multi-path services) • Inherent technology refresh services	
Network Attached Storage (NAS)	SAN-004	NAS (Network Attached Storage) brings scalability, reliability, and performance with storage volumes that can be connected to over the IP network. This service targets your file shares or where fibre channel connections aren't possible or practical and availability to support non-critical data. NAS addresses your network storage needs with basic performance and a very cost-effective solution	• Network addressable RAID 5 • Monitoring, configuration, control, and tuning software • Storage solution design with reliability, manageability, and scalability • Continuous operational support (24x7x365) • Volume adjustments, reallocation, or reconfiguration as needed supporting growth provisioning within 24 hours • Information availability of 99.0 percent	• A storage foundation able to take advantage of Information Lifecycle management • Utility reduces provisioning time to meet business demands • World-class managed services that satisfy your unique requirements • Consistent delivery, cost efficiency, operations service excellence, and peak technological innovation

Storage Service	SKU #	Description	Specifications	Benefits
			• Inherent technology refresh services	
Optional Storage Service	**SKU #**	**Description**	**Specifications**	**Benefits**
Managed Storage Tier 1, Mirrored Primary	ST-100	Managed Storage Tier 1 is designed for increased scalability and performance over the other SAN tiers. The package enables additional value by allowing volume adjustments, reallocation, or reconfiguration as needed supporting growth provisioning within 24 hours. Application profiles for this service include business applications and databases where higher performance is required.	• Highly scalable enterprise storage platform • RAID 0 + 1 • Monitoring, configuration, control, and tuning software • Storage solution design with reliability, manageability, and scalability • Increased ability to dynamically increase key service attributes (options) • Continuous operational support (24x7x365)	• A storage foundation able to take advantage of Information Lifecycle management • Reduced provisioning time to meet business demands • World-class managed services that satisfy your unique requirements • Consistent delivery, cost efficiency, operations service excellence, and peak technological innovation • Added redundancy and

Storage Service	SKU #	Description	Specifications	Benefits
		Mirrored primary offers enhanced performance and redundancy to the Service.	• Volume adjustments, reallocation, or reconfiguration as needed supporting growth provisioning within 24 hours • Information availability of 99.999 percent • Client multi-path services • Inherent technology refresh services	performance compared to standard Managed Storage Tier 1
Managed Storage Tier 1, with Local Clone Services, Mirrored Primary	ST-101	Managed Storage Tier 1 with Local Clone Services, Mirrored Primary is for mission-critical information and allows for continuous protection by means of non-disruptive Backup and Restore, that minimizes the impact of data protection on application availability and at the same time allows for better Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), thus meeting the	• RAID 0 + 1 primary disk, RAID 5 local clone • Integrated software, hardware, and managed services to provide the appropriate level of information protection by allowing for non-disruptive backups for database, application, and user data • Installation of system management and backup tool agent software as required	• Enhanced protection up to last synchronization point in case of loss of primary storage pool • Interval replication provides for a significant reduction of restore time through restore from recent disk replicas Use of an alternate host (client specified) provides for a minimum impact of backup on production processing through

Storage Service	SKU #	Description	Specifications	Benefits
		needs of the most demanding business applications. Data is replicated to separate primary storage at set intervals where the data is used for recovery purposes in case of hardware failures, or for additional backup and restore processing using a separate backup server for data movement. Through the use of additional business continuity volume (BCV) copies the non-disruptive solution in this sense does not use or impact production servers or data and provides information protection without causing an interruption to production. Non-disruptive backup services provide a LAN-less restore capability that leaves application hosts free to run your business. This service is available only within the Service	for the administrative server environment • Scheduling and management of local data replication processes for protection and recovery purposes • Support of custom scripts to enable non-disruptive backups to be performed	use of disk-based data replication to a separate device and storage pool • Added redundancy and performance compared to standard Managed Storage Tier 1

Storage Service	SKU #	Description	Specifications	Benefits
		Provider managed Data Centres		
Managed Storage Tier 1, Local Clone Services, Standard	ST-102	Managed Storage Tier 1 with Local Clone Services, Standard is for mission-critical information and allows for continuous protection by means of non-disruptive Backup and Restore, that minimizes the impact of data protection on application availability and at the same time allows for better Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), thus meeting the needs of the most demanding business	• RAID 5 primary disk, RAID 5 local clone • Integrated software, hardware, and managed services to provide the appropriate level of information protection by allowing for non-disruptive backups for database, application, and user data • Installation of system management and backup tool agent software as required for the administrative server environment	• The service enables you to replicate with a storage array, providing redundancy and minimize performace impacts • Enhanced protection up to last synchronization point in case of loss of primary storage pool • Interval replication provides for a significant reduction of restore time through restore from recent disk replicas • Use of an alternate host

Storage Service	SKU #	Description	Specifications	Benefits
		applications. Data is replicated to separate primary storage at set intervals where the data is used for recovery purposes in case of hardware failures, or for additional backup and restore processing using a separate backup server for data movement. Through the use of additional business continuity volume (BCV) copies the non-disruptive solution in this sense does not use or impact production servers or data and provides information protection without causing an interruption to production. Non-disruptive backup services provide a LAN-less restore capability that leaves application hosts free to run your business. This service is available only within the Service Provider managed Data Centres	• Scheduling and management of local data replication processes for protection and recovery purposes • Support of custom scripts to enable non-disruptive backups to be performed	(client specified) provides for a minimum impact of backup on production processing through use of disk-based data replication to a separate device and storage pool

Storage Service	SKU #	Description	Specifications	Benefits
Managed Storage Tier 1, with replication services, and local clone services (Mirrored Primary)	ST-103	Managed Storage Tier 1, with replication and local clone, Mirrored Primary is for mission-critical information and allows for continuous protection by means of non-disruptive Backup and Restore, that minimizes the impact of data protection on application availability and at the same time allows for better Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), thus meeting the needs of the most demanding business applications. Data is replicated to separate primary storage within a secondary data centre at set intervals where the data is used for recovery purposes in case of hardware failures, or for additional backup and restore processing using a separate backup server for data movement. Through	• RAID 0 + 1 primary, RAID 5 local clone (in both Data Centres) • Integrated software, hardware, and managed services to provide the appropriate level of information protection by allowing for non-disruptive backups for database, application, and user data • Installation of system management and backup tool agent software as required for the administrative server environment • Scheduling and management of local data replication processes for protection and recovery purposes • Support of custom scripts to enable non-disruptive backups to be performed • Replication of data from	• The service enables you to replicate to a single target site, providing the foundation for disaster recovery where geographic separation is a requirement.

Storage Service	SKU #	Description	Specifications	Benefits
		the use of additional business continuity volume (BCV) copies the non-disruptive solution in this sense does not use or impact production servers or data and provides information protection without causing an interruption to production. Non-disruptive backup services provide a LAN-less restore capability that leaves application hosts free to run your business. This service is available only within the Service Provider managed Data Centres	Service Provider Primary Site to Service Provider Secondary site via SRDF/Asynchronous replication	

Storage Service	SKU #	Description	Specifications	Benefits
Managed Storage Tier 1, with replication services and local clone services (standard)	ST-104	Managed Storage Tier 1, with replication and local clone, standard is for mission-critical information and allows for continuous protection by means of non-disruptive Backup and Restore, that minimizes the impact of data protection on application availability and at the same time allows for better Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), thus meeting the needs of the most demanding business applications. Data is replicated to separate primary storage within a secondary data centre in real time or at set intervals where the data is used for recovery purposes in case of hardware failures, or for additional backup and restore processing using a separate backup server for	• RAID 5 primary, RAID 5 local clone (in both Data Centres) • Integrated software, hardware, and managed services to provide the appropriate level of information protection by allowing for non-disruptive backups for database, application, and user data • Installation of system management and backup tool agent software as required for the administrative server environment • Scheduling and management allows for local and remote data replication processes for protection and recovery purposes • Support of custom scripts to enable non-disruptive backups to be performed • Replication of data from	• The service enables you to replicate to a single target site, providing the foundation for disaster recovery where geographic separation is a requirement.

Storage Service	SKU #	Description	Specifications	Benefits
		data movement. Through the use of additional business continuity volume (BCV) copies the non-disruptive solution in this sense does not use or impact production servers or data and provides information protection without causing an interruption to production. Non-disruptive backup services provide a LAN-less restore capability that leaves application hosts free to run your business. This service is available only within the Service Provider managed Data Centres	Service Provider Primary Site to Service Provider Secondary site via SRDF/Asynchronous replication	

Storage Service	SKU #	Description	Specifications	Benefits
Managed Storage Tier 1, with replication services (Mirrored Primary)	ST-105	Managed Storage Tier 1, with replication services is for mission-critical information and allows for continuous protection by means of replication that allows for better Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), thus meeting the needs of the most demanding business applications. Data is replicated to separate primary storage within a secondary data centre at set intervals where the data is used for recovery purposes in case of hardware failures. This service is available only within the Service Provider managed Data Centres. Mirrored primary offers enhanced performance and redundancy to the Service.	• RAID 5 primary, RAID 5 in secondary Data Centre • Integrated software, hardware, and managed services to provide the appropriate level of information protection by allowing for non-disruptive backups for database, application, and user data • Installation of system management and backup tool agent software as required for the administrative server environment • Scheduling and management allows for remote data replication processes for protection and recovery purposes • • Support of custom scripts to enable non-disruptive backups to be performed	• The service enables you to replicate to a single target site, providing the foundation for disaster recovery where geographic separation is a requirement.

Storage Service	SKU #	Description	Specifications	Benefits
			• Replication of data from Service Provider Primary Site to Service Provider Secondary site via SRDF/Asynchronous replication	
Managed Storage Tier 1, with replication services (Standard)	ST-106	Managed Storage Tier 1, with replication services is for mission-critical information and allows for continuous protection by means of replication that allows for better Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), thus meeting the needs of the most demanding business applications. Data is replicated to separate primary storage within a secondary data centre at set intervals where the data is used for recovery	• RAID 5 primary, RAID 5 in secondary Data Centre • Integrated software, hardware, and managed services to provide the appropriate level of information protection by allowing for non-disruptive backups for database, application, and user data • Installation of system management and backup tool agent software as required for the administrative server environment	• The service enables you to replicate to a single target site, providing the foundation for disaster recovery where geographic separation is a requirement.

Storage Service	SKU #	Description	Specifications	Benefits
		purposes in case of hardware failures. This service is available only within the Service Provider managed Data Centres	• Scheduling and management allows for remote data replication processes for protection and recovery purposes • • Support of custom scripts to enable non-disruptive backups to be performed • Replication of data from Service Provider Primary Site to Service Provider Secondary site via SRDF/Asynchronous replication	

Storage Service	SKU #	Description	Specifications	Benefits
Archive Storage Repository	ST-107	Archive Storage Repository Services are for Application specific archives (e.g. mail archive or database archive). The archive Storage Repository Services are designed to provide customers with ready access to archive storage. Management of the movement of data to the archive storage device including tools, processes, and people to define the archive policies and extract and retrieve of Data are the responsibility of the Province. Service Providers responsibilities are for the allocation of the storage and maintenance of the storage hardware.	• Secure environment • Continuous operational support (24x7x365) • Hardware availability of 99.7 percent • Inherent technology refresh services	• A storage foundation able to take advantage of Information Lifecycle Management • Data protected by replication of data in two geographically dispersed Data Centres •

Storage Service	SKU #	Description	Specifications	Benefits
File System Archive Storage Services	ST-108	File System Archive Storage Services is a compliment to Managed Storage Tier 1, Tier2 or Tier 3 for Windows Servers. The data contained in user home directories and group shares is a key area of focus. Basically, any data that is unstructured – meaning not under direct control of an application or database – is an area this service addresses. File System Archive Storage Services will provide a secure and cost-effective solution that reduces ongoing costs of file storage, improves file server management, optimizes backup/recovery cycles, and makes sure information can be retained and retrieved quickly and efficiently to meet compliance and management requirements. The service	• Automation of transparent data migration or archiving from primary storage to tiered archive storage • Continuous monitoring of file service environments and alerts on critical storage usage levels to proactively resolve capacity management issues • Automated file restores for files • Search capabilities for authorized users to locate, view, and retrieve archived files based on indexing • Secure environment • Continuous operational support (24x7x365) • Information availability of 99.7 percent • Inherent technology refresh services	• A storage foundation able to take advantage of Information Lifecycle Management • Data removed from primary storage and backup cycles • Data protected by replication of data in two geographically dispersed Data Centres

Storage Service	SKU #	Description	Specifications	Benefits
		requires analysis of the storage environment for data classification and policy definition purposes. Data is then targeted according to the Province policies for retention, and archived to the repository.		
Managed Storage Tier 2, Mirrored Primary	ST-109	Managed Storage Tier 2, Mirrored Primary provides scalability, reliability, and performance at an economical entry point for SAN storage. This service targets midrange environments, offering mid tier availability for Province data. Mirrored primary offers enhanced performance and redundancy to the Service.	• RAID 0 + 1 • Monitoring, configuration, control, and tuning software • Storage solution design with reliability, manageability, and scalability • Continuous operational support (24x7x365) • Volume adjustments, reallocation, or reconfiguration as needed supporting growth provisioning within 24 hours	• A storage foundation able to take advantage of Information Lifecycle Management • Utility service that reduces provisioning time to meet business demands • World-class managed services that satisfy your unique requirements • Added redundancy and performace compared to standard Managed Storage Tier 2

Storage Service	SKU #	Description	Specifications	Benefits
			• Information availability of 99.99 percent • Client multi-path services • Inherent technology refresh services	

Managed Backup Services	SKU #	Description	Specifications	Benefits
VTL Backup Services With Replication to Secondary Site	BK-001	Backup to local EDL, then replicate EDL at secondary site	• A complete backup set is created and retained on Virtual Tapes in a Virtual Tape Library (VTL) with a copy created at a secondary Data Centre. • Integrated software, hardware, and managed services to provide the appropriate level of information protection by providing centralized backups to a disk-based library for servers located in the two Data Centres. • Hardware, software, and connectivity required to attach local servers to centralized backup storage infrastructure, consisting of installation of system management and backup tool agent software as required for the administrative server environment • Provides information protection for direct attached, SAN and NAS connected primary storage	• Data is protected in two Data Centres • Enhaced speed for for backup and restore data transfers due to disk technology • RAID protected storage for virtual tape images providing improved data integrity • Improved RTO because of avoidance of physical tape mount and positioning delays • Enhanced reliability of disk-based data protection processes and storage. Facilitates improved availability of backup data • Reduced application downtime through an

Managed Backup Services	SKU #	Description	Specifications	Benefits
			• Automated scheduling of backup requirements, through Netbackup internal scheduler • Basic backup, and restore monitoring • NetBackup database agents to allow backups to run while databases remain up • Technology refresh services to maintain technology currency • Maximum of 2 Business Hour restore initiation of data	enhanced restore capability

Optional Backup Services	SKU #	Description	Specifications	Benefits
VTL Backup To Encrypted Offsite Tape	BK-100	Virtual Tape Backup to tape is a backup and recovery service that provides for enhanced data protection for Province Servers. Only the current Data Backup resides on the local VTL before being duplicated to and encrypted to tape to be stored at an offsite location. This approach to Data Backup will be used as the standard service during the period when only the Calgary Data Centre is Operational.	• A complete backup set is created and retained on Virtual Tapes in a Virtual Tape Library (VTL) with a physical encrypted tape copy created and sent offsite for Disaster Recovery and long term retention. • Integrated software, hardware, and managed services to provide the appropriate level of information protection by providing centralized backups to a disk-based library for servers located in the two primary centres. • Hardware, software, and connectivity required to attach local servers to centralized backup storage infrastructure, consisting of installation of system management and backup	• Disk speed for backup data transfers • RAID protected storage for virtual tape images for improved data integrity • Enhanced reliability of disk-based data protection processes and storage make sure of availability of backup data

Optional Backup Services	SKU #	Description	Specifications	Benefits
			tool agent software as required for the administrative server environment • Provides information protection for direct attached, SAN and NAS connected primary storage • Automated scheduling of backup requirements, through NetBackup internal scheduler • Basic backup, and restore monitoring • Tape media to meet backup requirements for a single, physical copy of backup data offsite. • Encryption on write to tapes, which are then stored Off-site • NetBackup database agents to allow backups to run	

Optional Backup Services	SKU #	Description	Specifications	Benefits
			while database remain up. • Technology refresh services to maintain technology currency	
Extended Retention Services	BK-101	Retention of backup tapes greater than 90 days. Retention term defined by Client. Data is duplicated on to physical tape and is stored onsite at the secondary Data Centre.	• After a complete backup set is created and retained on Virtual Tapes in a Virtual Tape Library (VTL) a physical encrypted tape copy is created for Disaster Recovery and long term (greater than 90 days) retention. • Integrated with both optional and base backup solutions • Hardware, software, and	• Provides secure data retention option for Clients who wish to retain data for langer than 90 days • Mirrored primary offers enhanced performance and redundancy to the Service. Restore times minimized having tape at Service Providers secondary Data Centre

Optional Backup Services	SKU #	Description	Specifications	Benefits
			connectivity required to attach local servers to centralized backup storage infrastructure, consisting of installation of system management and backup tool agent software as required for the administrative server environment • Tape media to meet backup requirements for a single, physical copy of backup data offsite. • Encryption on write to tapes • Technology refresh services to maintain technology currency	

Managed Mainframe Services

Managed Mainframe Services comprise monitoring, maintaining and managing the Mainframe Hardware and Mainframe System Software configurations, including acquisition, installation, configuration, management, testing support and disposal of all such hardware and system software. As per the SOW, the Province is responsible for the license fees and maintenance support fees to the applicable third party software vendors for the Non-Standard Software for which the Province is the licensor.

Mainframe Services

Mainframe Services include those services that are not listed as optional mainframe services.

MAINFRAME SERVICES	SKU #	Unit of Measure	Type	One-time Unit Price	Monthly Unit Price
Mainframe Processing Services	MFMIP-001	Per MIPS	Monthly	N/A	N/A
Mainframe Non-Standard Software	MFSW-001	Fixed	Monthly	N/A	N/A
Mainframe DASD Storage	MFDASD-001	Per GB	Monthly	N/A	N/A
Mainframe Tape Storage	MFBKUP-001	Per GB	Monthly	N/A	N/A

Pricing Example:

Mainframe Services based on 617 MIPS with 3,525 gigabytes of DASD and 145,000 gigabytes of tape would generate the following pricing configuration.

617 MIPS – Mainframe Processing Services MIPS
3,525 GBs – Mainframe DASD
1 – Mainframe Non-standard Software
145,000 GBs– Mainframe Tape

Managed Mainframe Services Optional Services

MAINFRAME OPTIONAL SERVICES	SKU #	Unit of Measure	Type	One-time Unit price	Monthly Unit Price
Form/Print/end user Support		Monthly	Monthly	N/A	N/A
SAS 70 Audit		Each Occurrence	Fixed Fee	N/A	N/A
Extended Database Management Services		Hourly Rate	Hourly	N/A	N/A
Database Administration	MFDB-100	Hourly Rate	Hourly	N/A	N/A
Database Production Support	MFDB-200	Hourly Rate	Hourly	N/A	N/A
Database Consulting Services	MFDB-300	Hourly Rate	Hourly	N/A	N/A
Extra Disaster Recovery Test	MFDRT-100	Each Occurrence	Fixed Fee	N/A	N/A

SCHEDULE 24

PRIVACY OBLIGATIONS

(Section 16.1)

1. General Purpose

The purpose of this **Schedule 24** (*Privacy Obligations*) and Appendix A hereto, is to set forth the obligations of Service Provider relating to the protection of Personal Information to ensure that the Personal Information is not collected, used or disclosed other than as may be permitted under the Applicable Laws (including the *Freedom of Information and Protection of Privacy Act* (British Columbia)) and subject to complying with Applicable Laws: (i) in the ordinary course of providing the Services, provided such disclosure is within Canada; (ii) as set out in Article 16 (*Privacy, Security and Confidentiality*) of the Agreement; (iii) as may be directed by the Province under Section 5 of this Schedule; or (iv) strictly in accordance with policies or procedures expressly approved by the Province (collectively, the "**Privacy Obligations**").

2. Acknowledgements

The Parties acknowledge that:

(a) the Personal Information includes information that the Province is obligated to protect pursuant to privacy legislation and the Personal Information is highly sensitive confidential information;

(b) the Personal Information includes health related records and other Personal Information to which Service Provider has been provided access and/or Custody under the terms of the Agreement;

(c) the Province has Control of the Personal Information in order that the Province may serve the public;

(d) the Personal Information is collected, used, disclosed, and otherwise managed by the Province on behalf of the public;

(e) this Schedule is premised on the Province's commitment as the owner and controller of the Personal Information and Service Provider's commitment as a service provider to the Province, as contemplated in the *Freedom of Information and Protection of Privacy Act* (British Columbia) and the Agreement, to maintain the privacy and security of the Personal Information; and

(f) nothing in this Schedule shall require Service Provider or any Subcontractor to act contrary to Applicable Law.

3. Service Provider Commitment

In order to protect Personal Information while in the Custody of Service Provider, the Province has required the Service Provider's commitment, and Service Provider has committed, to comply with the Privacy Obligations. The Service Provider shall develop and maintain policies and procedures specific to the privacy and security of the Personal Information as described in Appendix B (*Privacy Management Plan*) to this **Schedule 24** (*Privacy Obligations*), and the Service Provider will maintain current policies

and procedures which will, at all times, be consistent with the Agreement and this **Schedule 24** (*Privacy Obligations*).

4. Conflicts

Notwithstanding the provisions of Section 1.11 of the Agreement (*Document Conflicts*), if there is a conflict or inconsistency between this **Schedule 24** (*Privacy Obligations*) and the provisions of the Agreement or any other Schedule attached to the Agreement, then the provisions of this **Schedule 24** (*Privacy Obligations*) shall govern.

5. Directives

The Province, through its Designated Representative, may at any time, in accordance with Section 11.4 (*Province's Right to Issue Directives*) of the Agreement, amend these Privacy Obligations upon reasonable prior written notice (under the circumstances) to Service Provider. Such amendments shall be implemented in accordance with the Change Order Process.

6. Non-Disclosure of Personal Information

Service Provider shall not disclose the Personal Information to any Person for any reason other than as permitted in accordance with Applicable Laws (including the *Freedom of Information and Protection of Privacy Act* (British Columbia) and, subject to complying with Applicable Laws: (i) as contemplated pursuant to Article 16 (*Privacy, Security and Confidentiality)* of the Agreement; and (ii) in the ordinary performance of the Services in accordance with the SOW Documents. Without limiting the generality of the foregoing, Service Provider shall not disclose any Personal Information pursuant to a Disclosure Order, as more expressly limited pursuant to Section 16.2 *(Foreign Disclosures)* of the Agreement.

7. Anticipatory Disclosure of Personal Information

Where the Province determines, acting reasonably, that there is a risk that the Personal Information may be disclosed contrary to the terms of this Agreement, then the Province, through its Designated Representative, shall have the right and authority to take all actions necessary to prevent such disclosure including, without limitation, any one or more of the following:

(a) requiring that the Service Provider immediately revoke the right of access to Personal Information of such Authorized Personnel posing such risk that Personal Information may be disclosed;

(b) proceeding directly to court in respect of such potential disclosure, as more particularly contemplated in Section 25.1 *(General Intent)* of the Agreement;

(c) temporarily replacing any Personnel or other applicable Service Provider employees in order to allow the Province to take all actions necessary to prevent such disclosure provided that: (i) such replacement personnel shall have the same or substantially similar qualifications as the Service Provider Personnel or other applicable Service Provider employee being temporarily replaced and where no such replacement personnel is available, the Province shall have the right to appoint a monitor to observe such Service Provider Personnel and other applicable Service Provider employees; (ii) any such replacement personnel or monitor shall be appointed by the Designated Representative of the Province or, in that person's absence, by any Province Key Person designated by such person; (ii) the Province's right to temporarily replace or monitor any Personnel or other applicable Service Provider employees and the authority of any person appointed to do so

shall be restricted to the acts and limited to the time period reasonably necessary to prevent such disclosure. The Province shall give the Service Provider written notice of any temporary replacement or monitoring of Personnel or other Service Provider employees under this section and shall simultaneously provide Service Provider with written notice specifying the circumstances and grounds upon which the Province is relying in exercising its rights hereunder, in sufficient detail to enable Service Provider to assess and respond to the same. Notwithstanding the foregoing, any such response from Service Provider shall not entitle Service Provider to prevent the Province from exercising its rights under this paragraph (c) (it being acknowledged by the Parties that Service Provider shall be entitled to bring its response forward through the dispute resolution process set forth in Article 27 (*Dispute Resolution*) of the Agreement should Service Provider reasonably believe that the Province did not have proper grounds for exercising its rights under this paragraph). Notwithstanding the foregoing, nothing in this paragraph shall provide the Province with any right to inspect or access any Service Provider Confidential Information.

Where the Province intends to exercise its rights under Sections 7(c) above, then the Designated Representative shall, prior to such exercise, provide to the President of Service Provider or the next most senior Service Provider Key Position a written notice, which contains:

(a) the basis for belief that there is a risk that the Personal Information may be disclosed contrary to the terms of the Agreement;

(b) the period, if any, during which Service Provider may attempt to reasonably prevent the disclosure or remedy the risk;

(c) the general course of action that the Province proposes to take and any powers provided for in this Agreement that the Province proposes to exercise; and

(d) the expected length of time that this action is anticipated to take.

Upon receipt of such notice Service Provider shall notify the Designated Representative of the Province or, in that person's absence, any Province senior executive designated by such person of the actions that Service Provider will take to prevent the disclosure or remedy the risk where given the opportunity to do so. For the purposes of this **Schedule 24** (*Privacy Obligations*), the "**Designated Representative**" means a representative appointed by the Administrator.

8. Compliance Certificate

Service Provider shall deliver a Compliance Certificate to the Province every Contract Year within three (3) months after the end of a Contract Year, which confirms, among other things, Service Provider's, and the Access Subcontractors', compliance with Article 16 (*Privacy, Security and Confidentiality*) and this **Schedule 24** (*Privacy Obligations*) and any other similar obligations contained in the provisions of the Agreement. The Parties shall review each Compliance Certificate at the Joint Executive Committee within three months of the date of delivery of such certificate.

9. Flow Down of Obligations

(a) The obligations contained in the following sections of these Privacy Obligations shall be flowed down by Service Provider to any Access Subcontractors, to the extent applicable to each Access Subcontractor given the nature of the Services provided by it: 6, 10, 11, 12 (unless agreed otherwise by the Province through the Governance Process on a case

by case basis where a particular Access Subcontractor has adequate training and security measures in place), 13(b), 14, 15, 16, 17(a) – (c) (unless agreed otherwise by the Province through the Governance Process on a case by case basis where a particular Access Subcontractor has adequate security standards in place), 17(e) – (h), 17(j), 18, 19(a) – (i), 20, 21, 22, 23, 24(a), 25(a), 25(c)-(d), 26, 29 and 32 (as applicable to Access Subcontractors), 28(a) – (c), 31 (as applicable to Access Subcontractors), 34, 36, 37 (to the extent applicable), 39 (provided that notice be given by the Access Subcontractor to Service Provider and from Service Provider to the Province), 40 and 41.

(b) The obligations of the Service Provider under Section 9(a) above and under each of the sections referred to in Section 9(a) above are to be flowed down to Access Subcontractors.

10. Ownership and Control of Personal Information

The Province shall be and remain the exclusive owner of all right, title and interest in and to the Personal Information and shall be and remain in complete Control of the Personal Information. No access to or Custody of Personal Information by Service Provider or any other Person as contemplated in this Agreement shall be construed in any manner as providing Control or any other rights with respect to such Personal Information.

11. Privacy Management Plan

Service Provider shall develop and maintain plans, policies and procedures specific to privacy and security as described in Appendix B *(Privacy Management Plan)* to this **Schedule 24** *(Privacy Obligations)* and that include protocols and procedures to be followed in the event of a use or disclosure of Personal Information contrary to the provisions of the Agreement or this **Schedule 24** (*Privacy Obligations*). Service Provider shall make such policies and procedures available for review (at Service Provider's premises) by the Province, upon the request of the Province from time to time. Service Provider shall advise the Province through the Governance Process of any material changes that it makes to such policies and procedures.

12. Training

Service Provider shall maintain and provide training of all Authorized Personnel in the following areas (and provided that, with respect to External Personnel who are Authorized Personnel, the Service Provider shall maintain and provide such training or shall require the Access Subcontractor who employs such External Personnel to do so):

(a) relevant aspects of privacy and security including those set forth in these Privacy Obligations as may be appropriate to their job function;

(b) in respect of any Authorized Personnel relevant aspects of collection, storage, release, disposal and security of the Personal Information as appropriate; and

(c) the hotline established by the Province (telephone number 250-356-1851) from time to time in order that the Authorized Personnel can notify the Province directly in the event of any unauthorized disclosure or potential unauthorized disclosure of Personal Information.

Service Provider shall provide refresher training to Authorized Personnel in respect of the foregoing, annually or, more frequently where necessary to implement material changes in the applicable policies or

procedures. Service Provider shall develop and maintain staff manuals that detail the security and privacy procedures that are applicable to all Authorized Personnel.

The Service Provider shall provide all Transitioning Employees with training, as set forth in this Section 12 (*Training*), within two weeks after the Effective Date.

13. Privacy Impact Assessments/Threat and Risk Assessments

During the Term of the Agreement, the Service Provider shall conduct a security threat and risk assessment in accordance with Section 15 below:

(a) at each Service Location prior to the provision of Services from a Services Location, using a checklist derived by Service Provider from ISO27002;

(b) prior to any material change in the Services, procedure, applications or technology relating to or used in connection with Personal Information: and

(c) promptly in the event of a security incident,

and the Service Provider shall work cooperatively with the Province and assist the Province with the Province's preparation of a Privacy Impact Assessment. The Province shall have the right to review the results of all security threat and risk assessments and security audits undertaken by Service Provider and with respect to paragraphs (a) and (b) above, the Service Provider will not provide Services from any Service Location or implement any material change in the Services, procedure, applications or technology relating to or used in connection with Personal Information unless and until the security threat and risk assessments and security audits have been completed to the satisfaction of the Province, acting reasonably. With respect to paragraph (c) above, the Service Provider may continue to provide Services from the Service Location while the security threat and risk assessment is undertaken by the Service Provider, and completion of the security threat and risk assessment is subject to the satisfaction of the Province, acting reasonably. Notwithstanding the foregoing, the Province has the right to conduct, at its own expense, its own Privacy Impact Assessments and security audits under Article 15 (*Audit Rights*), in respect of the foregoing.

14. Testing and Development Work

The Service Provider shall not use Personal Information or personally identifiable data of the Province for any non-production purpose including, without limitation, application testing, development, maintenance and training environments.

15. Risk Assessment

Service Provider shall, throughout the Term (as applicable):

(a) conduct a threat and risk assessment using a checklist derived by Service Provider from ISO27002 (as revised and replaced from time to time), and shall provide a copy of the results thereof to the Province prior to implementation of any material technology changes or material business transformation changes; and

(b) cooperate with the Province in conducting SysTrust Audits or SAS 5970 Audits as contemplated by Section 22.6 (*SysTrust Report*) of the Agreement.

Notwithstanding the foregoing, the Province shall have the right to conduct, at its own expense, its own risk and control reviews or other security reviews to its satisfaction. Any such risk and control reviews or other security reviews shall be considered as audits carried out pursuant to and subject to the provisions of Article 22 (*Audit Rights*) of the Agreement and shall in no way limit or otherwise diminish Service Provider's obligation to comply with the Privacy Obligations and other provisions of the Agreement.

16. Removal of Personal Information

Service Provider acknowledges that the Authorized Personnel shall at no time be provided with the ability or authority to remove Personal Information from the Service Locations unless the purpose for such removal is expressly authorized elsewhere in these Privacy Obligations or in the Agreement (including in Appendix B (*Privacy Management Plan*) to this **Schedule 24** (*Privacy Obligations*)), or as otherwise agreed between the Parties.

17. Security Generally

Service Provider shall make arrangements to maintain the security of the Personal Information that is in its Custody, or that it otherwise has access to, by protecting the Personal Information against such risks as unauthorized access, collection, use, duplication, modification, disclosure, storage or disposal. In particular, Service Provider shall:

(a) meet or exceed the codes of practice for information security management outlined in ISO27002 (as revised and replaced from time to time);

(b) meet or exceed the security policies, standards, guidelines and practices of the Province as outlined and implemented in:

(i) the Province's Core Policy Manual, particularly sections 12 and 15 thereof , as may be applicable to the Service Provider as a service provider to the Province and as may be relevant to the performance of the Services by the Service Provider (http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm); and

(ii) the Information Technology Security Policy (http://www.cio.gov.bc.ca/Services/Security/ISP.asp),

as the same may be amended, revised or replaced from time to time pursuant to the Change Order Process (the Parties acknowledge that copies of the above documents, dated the Effective Date, have been provided by the Province to the Service Provider concurrently with the execution of the Agreement);

(c) assess and adopt privacy and security enhancing technologies and cryptographic controls over the Term to improve security and restrict access to Personal Information to Authorized Personnel, as approved and implemented in accordance with the Change Order Process;

(d) follow Directives from the Province from time to time in accordance with Section 11.4 (*Province's Right to Issue Directives*) of the Agreement with respect to security requirements in accordance with the Change Order Process;

(e) have in place all necessary network controls and other security to maintain the level of security required for the Personal Information being handled;

(f) require that all storage of Personal Information, including Personal Information in the Custody of Service Provider, shall remain at all times in Canada in accordance with the terms of the Agreement;

(g) require that any Personal Information be removed from Service Provider's or its Access Subcontractors' systems, physical storage areas, storage devices (including removable media, back-up media and materials) upon the Termination of the Agreement, within an agreed period of time, and in accordance with the termination provisions under Article 28 (*Termination Assistance*) of the Agreement;

(h) require that the equipment and telecommunications facilities used by Service Provider or its Subcontractors in the delivery of the Services (which are owned by or otherwise in the custody or control of Service Provider or its Subcontractors) which host, transmit, Store or otherwise make available any Personal Information are secured by, for example, an electronic card access system, combination lock, lock and key, or other similar physical security measure;

(i) require the currency of critical software such as installation of patches and virus software updates on a timely basis, and the proactive monitoring of vendor alert services; and

(j) manage the Services and monitor the Authorized Personnel to prevent and detect security breaches such as unauthorized access to Personal Information, and incorporate procedures to require that all access to Personal Information is given only to Authorized Personnel and Authorized Users, and to promptly revoke access to any such Persons when no longer required.

18. Physical and Environmental Security

Service Provider shall develop, maintain and enforce policies that require, throughout the Term:

(a) Data rooms where Personal Information is Stored (collectively, the "**Secured Facilities**"), shall have appropriate physical and environmental security controls such as air conditioning, UPS/power generators, surge protection, fire protection or other similar measures, where **"Store"** or **"Storage"** means storage of Personal Information except for storage on a temporary basis such as caching for ephemeral or immediate processing purposes;

(b) all access to the Secured Facilities is restricted and monitored. In addition to the other obligations set forth in the Agreement and these Privacy Obligations, Service Provider shall require that the Secured Facilities have adequate physical security controls such as keys, entry cards or other similar controls; and

(c) except as set forth in Section 19(h) below, or otherwise by mutual agreement of the Parties in writing, Authorized Personnel are prohibited from bringing into or removing from the Secured Facilities any electronic data storage devices that may be used to copy or transport any Personal Information.

19. Secured Databases

Service Provider shall develop, maintain and enforce policies, standards and guidelines relating to Service Provider controlled Systems and Service Provider Managed Systems (defined below) that Store Personal Information ("**Secured Databases**"). Secured Databases do not include workstations or Systems that

have access to but do not Store Personal Information, except as agreed to by both Parties. Service Provider's policy shall:

(a) require that no Personal Information is stored by Authorized Personnel on laptops, PDAs, or any other mobile computing devices unless authorized under or pursuant to the terms of the Agreement or otherwise approved by the Province;

(b) identify all Secured Databases including, where applicable, serial numbers;

(c) protect Secured Databases in accordance with the authentications standards set forth in Section 20 *(Authentication Project and Standards)* below;

(d) authorize and control any and all remote access to Secured Databases such that:

(i) with respect to Service Provider controlled Systems, no Secured Databases may be connected to the Internet or to any wide area network except as protected by firewalls, application servers and other appropriate security controls,

(ii) with respect to Service Provider controlled Systems, no Secured Databases may be hosted on hardware that also hosts email, Internet, wireless or other wide area server applications, or other generally accessible local area server applications, and for greater clarification, Service Provider shall not store any Secured Databases on a Microsoft exchange server or other servers of similar functionality,

(iii) Authorized Personnel who require remote access to Secured Databases may access such Secured Databases remotely for the purpose of performing maintenance and emergency maintenance on the Systems used in the performance of the Services, in accordance with the following restrictions:

(A) remote access to Secured Databases will only be permitted through a personal computer, terminal or laptop that is subject to the Service Provider's usage and security policies and that it equipped with the most current security features and software as required by the Service Provider's policies (for greater clarity, "usage" of the personal computer, terminal or laptop will be limited to Authorized Personnel),

(B) remote access to the Secured Databases will only be possible using Secure Socket Layer (SSL) and Virtual Private Network (VPN) technology based secure internet access to the Secure Database location, as Approved by the Province;

(e) require that an Service Provider firewall is in place between Service Provider owned and operated networks storing Secured Databases and other networks such as SPAN/BC;

(f) except as expressly set forth in this **Schedule 24** (*Privacy Obligations*) of the Agreement, provide that there shall be no remote access to any Secured Databases;

(g) require that Secured Databases are not removed from Secured Facilities except as expressly authorized in this **Schedule 24** (*Privacy Obligations*)) (including in Appendix B (*Privacy Management Plan*), or as otherwise agreed between the Parties;

(h) require that all Secured Databases shall not have any active writeable/recordable removable data storage devices (such as floppy drives, CD or DVD burners), and all USB or other ports to which external storage devices (such as external hard drives) may be connected must be disabled for such use, except where required to perform the Services such as:

(i) for authorized back-up of Personal Information,

(ii) for the purposes of software updates, maintenance and emergency maintenance and where the Authorized Personnel performing such software updates, maintenance and emergency maintenance use a personal computer, terminal or laptop that is subject to the Service Provider's usage and security policies and that it equipped with the most current security features and software as required by the Service Provider's policies (for greater clarity, "usage" of the personal computer, terminal or laptop will be limited to Authorized Personnel) and shall be restricted by credentials, including password, protected using physical security measures that prohibit use of the media or access to the Personal Information contained thereon, and the Personal Information contained thereon shall be encrypted using cryptography that meets or exceeds the adopted cryptography standards of the Province as of the Effective Date;

(i) require that all storage devices used in Secured Databases or otherwise containing Personal Information will be disabled prior to removal from the Secured Facilities, in accordance with the provisions of the Security SOW (except as the Parties have expressly agreed otherwise with respect to the Remote Infrastructure Server Locations and the Remote Application Server Locations), and destroyed (using secure destruction and disposal mechanisms) strictly in accordance with Province Policy. For greater clarity, the Service Provider may only redeploy storage devices used in Secured Databases or otherwise containing Personal Information in connection with the provisions of the Services to the Province and not in connection with the provision of services to any third party, including any Broader Public Sector entities; and

(j) require that any processing systems used to provide the Services that are shared with other clients of Service Provider or any Access Subcontractor are partitioned in such a way to allow only Authorized Personnel to access any Personal Information.

These protected networks include, without limitation, the approved service locations specified in **Schedule 8** (*Service Locations*) of the Agreement.

For purposes hereof:

(a) "**remote access**" means access to Secured Databases from locations other than the Service Locations set forth in **Schedule 8** (*Service Locations*).

(b) "**Service Provider Managed Systems**" means Systems that are owned by the Province as of the Hand-Over Date, and for which the Service Provider is responsible to manage in the performance of the Services, from and after the Hand-Over Date.

20. Authentication Project and Standards

Service Provider acknowledges that the Province is currently undertaking an authentication project, and that Service Provider shall be required to comply with the Province's authentication requirements as a

result of such project to the extent that the same relates to the Services or otherwise to the Personal Information, which requirement shall be brought forward to Service Provider through the Change Order Process. Service Provider shall develop, maintain and enforce policies, standards and guidelines that require of all Systems controlled by Service Provider:

(a) credentials and other mechanisms, including passwords to restrict access to Personal Information;

(b) strong and unique user IDs and credentials, including passwords assigned to individual Authorized Personnel;

(c) power-on and screen-saver passwords and session time-outs (as appropriate);

(d) authentication, credential and password rules that meet or exceed the Province's standards, including standards relating to character length and time-expiry of passwords; and

(e) other similar measures.

21. Internet and Email

Service Provider shall develop, maintain and enforce policies, standards and guidelines governing Authorized Personnel who have access to the Internet or to outbound email from the workstations in which they access Personal Information, in particular, restricting the linking of any Personal Information to the Internet or to outbound email, restricting such access to Authorized Personnel who specifically require Internet or outbound email from their workstations to perform their job functions, and requiring that all such Internet or email access shall be subject to logs that enable Service Provider and, where appropriate, the Province to identify the time and connection details of any Internet and email activities of Authorized Personnel.

22. Wireless Network Controls

The Service Provider shall not use any wireless networks (owned or operated) in the performance of the Services:

(a) as part of local area networks implemented by the Services Provider in the Province Data Centres, the Remote Infrastructure Server Locations and the Remote Application Server Locations; and

(b) as part of local area networks implemented at the STMS Data Centres,

except with the prior Approval of the Province or in accordance with Province Policies relating to the use of wireless networks as may be implemented by the Province after the Hand-Over Date.

23. Transmission and Back-ups of Personal Information

Service Provider shall develop, maintain and enforce policies, standards and guidelines that require that throughout the Term all individual items of hardware or storage media that Store Personal Information that are permitted or required, pursuant to the Agreement or to these Privacy Obligations, to be removed from Secured Facilities ("**Secured Media**"), may only be removed for purposes such as off-site back-up and business continuity, destruction or at the express direction of the Province, in writing. Access to Secured Media shall be restricted by credentials, including password, protected using physical security

measures that prohibit use of the media or access to the Personal Information contained thereon, and the Personal Information contained thereon shall be encrypted using cryptography that meets or exceeds the adopted cryptography standards of the Province as of the Effective Date, with the exception of the Managed Backup Services described in the Storage and Backup SOW.

24. Secured Media Records

Service Provider shall develop, maintain and enforce policies, standards and guidelines that require that records are maintained as necessary to:

(a) identify all Secured Media (identified by unique catalogue or serial number); and

(b) identifying the location of the Secured Media.

25. System Logs

Service Provider shall record and maintain user access records/logs ("**System Logs**") with respect to all electronic Personal Information for the purpose of audit and investigations by the Province. Service Provider shall require that Service Provider developed applications with Personal Information shall conform to paragraphs (a) – (c) below, and that any applications delivered to Service Provider that support an audit trail shall continue to have such support. S. 15

S. 15

S. 15

S. 15

S. 15 . Thereafter the Service Provider shall deliver such System Logs to the Province unless the Parties agree otherwise in writing by the Province. The Service Provider shall make information from such System Logs available to the Province, in a timely manner and in accordance with **Schedule 21** (*Reporting Requirements*) and otherwise, at the cost of the Province from time to time, upon request.

The Parties acknowledge that as technology evolves during the Term of the Agreement, there may be other Data that the Province will require the Service Provider to log. Such Province request will be subject to the Change Order Process.

26. Notification

Service Provider shall develop, maintain and enforce policies, standards and guidelines that require that the Service Provider developed systems that Store or provide access to Personal Information shall have mechanisms in place to provide notification to a Person or Persons designated by the Province through the Governance Process in the event of specific irregular actions such as unauthorized access, security malfunction, irregular access, large scale copying or other similar activities with respect to Personal Information. For purposes thereof, Service Provider shall require that its Access Subcontractors report any such irregular actions to Service Provider, and Service Provider shall report the same forthwith to the Province in accordance with the foregoing.

27. Organizational Security

Service Provider shall throughout the Term:

(a) have clearly defined security roles and responsibilities within Service Provider in the form of organization charts and role descriptions for specialized security personnel;

(b) ensure appropriate security requirements are included in all of its Subcontractor contracts entered into in connection with providing the Services;

(c) have a designated Privacy, Security and Compliance Officer, who is not a US Personnel (defined below), responsible for monitoring and enforcing privacy and security measures and who is responsible for implementing the Directives of the Province pursuant to Section 11.4 *(Province's Right to Issue Directives)* and in accordance with the terms of the Agreement; and

(d) have an individual who is not a US Personnel (defined below) act in administrator roles with elevated access privileges, such as Systems Administrator, Network Administrator, Database Administrator, Security Administrator or Applications Administrator or other similar positions.

28. Limiting Access to Authorized Personnel

Except as expressly permitted in the Agreement or as expressly approved by the Province, and subject to any additional requirements set out in the Agreement, Service Provider shall require that the Personal Information may be accessed only by individuals who:

(a) are Personnel who are employees of Service Provider who have entered into a Confidentiality Covenant (as defined below), Independent Contractors or employees of the Access Subcontractors or Access Subcontractor's Affiliates who have entered into an External Confidentiality Covenant (as defined below), or other External Personnel of an Access Subcontractor who have entered into an agreement as contemplated in Section 31 (*External Confidentiality Covenant*) of this **Schedule 24** (*Privacy Obligations*); and

(b) are not US Personnel; and

(c) have a need to access the Personal Information in order to perform their job tasks (provided that such job tasks are in furtherance of the Services and are not inconsistent with the terms or the purpose of these Privacy Obligations)

(the "**Authorized Personnel**")

29. Monitoring of Telephone Calls

Service Provider shall restrict telephone monitoring to Authorized Personnel and will require that any Personal Information obtained from such monitoring is:

(a) not Stored at any location other than those locations permitted under **Schedule 8** (*Service Locations*) of the Agreement; and

(b) only used by or disclosed to Authorized Personnel. Service Provider shall maintain and enforce policies that prohibit the use or disclosure of any sensitive monitored information by its Authorized Personnel.

30. Confidentiality Covenant

All Personnel who require access to Personal Information shall be required to sign confidentiality covenants in a form approved by the Province (the "**Confidentiality Covenants**") attached as Appendix C and Appendix D to this **Schedule 24** (*Privacy Obligations*). The Confidentiality Covenants shall contain non-disclosure obligations along with express obligations to advise the Service Provider directly in the event that the Person becomes aware of any disclosure or potential disclosure of Personal Information. Service Provider shall not permit any Personnel to engage in any activities with respect to the Services or the Agreement nor have any access to Personal Information until such time as a Confidentiality Covenant has been signed and delivered by the Personnel to Service Provider. Upon the request of the Province, Service Provider shall confirm, in writing, to the Province that all Personnel who require access to Personal Information have signed a Confidentiality Covenant. The form of Confidentiality Covenant in effect at the Effective Date is attached to as Appendix C this **Schedule 24** (*Privacy Obligations*). Any change in the form of a Confidentiality Covenant implemented after the Effective Date shall be implemented in accordance with the Change Order Process. Service Provider shall cause all Personnel to reconfirm in writing their Confidentiality Covenant on an annual basis.

31. External Confidentiality Covenant

All External Personnel who are: (i) Independent Contractors; (ii) employees of Access Subcontractors or Access Subcontractor's Affiliates; and (iii) employees of such new Material Subcontractors as may be requested by the Province from time to time (acting reasonably but having regard to all of the surrounding circumstances); and who have access to Personal Information shall be required to sign External Confidentiality Covenants in a form approved by the Province (the "**External Confidentiality Covenant**"). The External Confidentiality Covenant shall contain non-disclosure obligations along with express obligations to advise the Access Subcontractor, new Material Subcontractor or Affiliate, as the case may be, directly in the event that the External Personnel becomes aware of any disclosure or potential disclosure of Personal Information. Service Provider shall not permit any such External Personnel to have any access to any Personal Information until such time the relevant External Personnel referred to above in this section have signed an External Confidentiality Covenant and all such signed agreements have been delivered to Service Provider. Upon the request of the Province, Service Provider shall confirm, in writing, to the Province that all External Personnel who require access to Personal Information have signed an External Confidentiality Covenant. The form of External Confidentiality Covenant in effect at the Effective Date is attached as Appendix D to this **Schedule 24** (*Privacy Obligations*). Any change in the form of External Confidentiality Covenant implemented after the Effective Date will be implemented in accordance with the Change Order Process. Service Provider shall require that all External Personnel who are required by this paragraph to sign an External Confidentiality Covenant shall reconfirm in writing their External Confidentiality Covenants on an annual basis.

32. Precedence of Personnel Agreements/Whistleblower Protection

Service Provider shall include in its employee agreements with its Personnel or supplement its employee agreements with its Personnel with the specific language with respect to privacy and confidentiality of the Personal Information, which language may take the form of a unilateral agreement by Service Provider to the Personnel. The language in the attached Appendix C shall provide for precedence for the Confidentiality Covenant pertaining to the obligation to protect privacy and confidentiality of Personal Information over any agreement that Service Provider has with the Personnel.

The Service Provider will not dismiss, suspend, demote, discipline, harass or otherwise disadvantage Personnel (including, for greater certainty, Authorized Personnel), or deny that Personnel (including, for greater certainty, Authorized Personnel) a benefit, because the individual acting in good faith and on the basis of reasonable belief: (a) has notified the Province of a foreign demand for disclosure; (b) has otherwise disclosed to the Province that the Service Provider has contravened or is about to contravene the *Freedom of Information and Protection of Privacy Act* (British Columbia); (c) has done or stated an intention of doing anything that that is required to be done in order to avoid having any person contravene the *Freedom of Information and Protection of Privacy Act* (British Columbia); (d) has refused to do or stated an intention of refusing to do anything that is in contravention of *Freedom of Information and Protection of Privacy Act* (British Columbia); or (e) the Service Provider believes that Personnel (including, for greater certainty, Authorized Personnel), will do anything described in this Section 32 (a) – (d).

33. Security Clearances

Service Provider shall perform or cause to be performed security clearances in connection with any sensitive information that Service Provider may obtain access to in the course of providing the Services. At the request of the Province, acting reasonably, and in accordance with the Change Order Process, Service Provider shall perform or cause to be performed security clearances for other Authorized Personnel who will have access rights to Personal Information prior to the time at which such Authorized Personnel first access Personal Information in connection with the Services. The scope of the Authorized Personnel subject to security clearances and the nature of the security clearances conducted on such individuals shall be as agreed to between the Parties pursuant to the Governance Process, or as may be otherwise required in accordance with any Applicable Laws. For the purposes of this **Schedule 24** (Privacy Obligations), the term "security clearance" shall mean: (a) verification of personal data, educational, professional and qualifications data and references; (b) a check of criminal records; and (c) a Canadian Police Identification Centre ("**CPIC**") Level 1 and Persons CPIC query.

34. US Personnel

Subject to Applicable Laws, no Personnel or External Personnel who are US Personnel shall have any access to Personal Information at any time unless required and expressly approved in advance by the Province pursuant to the terms of the Agreement or otherwise. Where US Personnel are required for the performance of the Services, Service Provider shall provide dummy data to the extent possible, such as by replacing Personal Information (such as names, phone numbers and addresses) with identifiers, or utilizing other means as reasonably directed by the Province through the Governance Process. Any approved US Personnel shall only access Personal Information from an approved service location specified in **Schedule 8** *(Service Locations)* attached to the Agreement. Under no circumstances shall any US Personnel:

(a) have remote access to Personal Information; or

(b) be permitted at any time to copy, export or otherwise remove or send any Personal Information from an approved service location specified in **Schedule 8** *(Service Locations)* attached to the Agreement.

US Personnel shall only be permitted to: (i) access or request Personal Information, or (ii) access a Secured Database, when escorted and generally supervised by or in the company of Authorized Personnel.

35. Paramountcy of Obligation to Protect Personal Information

Service Provider acknowledges that its applicable policies, education and training of Authorized Personnel, shall reflect the obligations of the Personnel pursuant to the Confidentiality Covenants and the External Confidentiality Covenants (as applicable), which may require them to act in a manner that is contrary to the interests of Service Provider (for example, because the fulfillment of such obligations may result in remedies being assessed against Service Provider under the terms of the Agreement). The Parties shall not, throughout the Term:

(a) discipline or discourage Authorized Personnel from acting in accordance with:

(i) provisions of the Confidentiality Covenant or the External Confidentiality Covenant pertaining to the protection of the privacy and confidentiality of the Personal information, or

(ii) Service Provider's obligations to the Province pursuant to these Privacy Obligations as implemented in accordance with Appendix B to this **Schedule 24** (*Privacy Management Plan*); or

(b) impose or permit to be imposed on any Authorized Personnel any obligation that is inconsistent with or that materially adversely affects his or her ability to fulfill:

(i) his or her obligations pursuant to a Confidentiality Covenant or External Confidentiality Covenant (as applicable), or

(ii) Service Provider's obligations to the Province pursuant to these Privacy Obligations as implemented in accordance with Appendix B to this **Schedule 24** (*Privacy Management Plan*).

36. Data Sharing

Except as may be permitted under Applicable Laws or as may be provided otherwise under the Agreement or the Transaction Documents, or as may be explicitly approved by the Province through the Governance Process, under no circumstances shall Service Provider enter into any relationship, contractual or otherwise, with any other Person involving data sharing or data access with respect to the Personal Information.

37. Collection of Personal Information

Except as may be provided otherwise in the Agreement or as may otherwise be directed by the Province in writing pursuant to the Governance Process, Service Provider shall not collect or create any Personal Information in the performance of the Services (other than Personal Information that is necessary for the performance of Service Provider's obligations, or the exercise of Service Provider's rights, under the

Agreement). Except as otherwise contemplated or permitted in the Transaction Documents, Service Provider shall:

(a) collect such Personal Information directly from the Person to whom the Personal Information relates;

(b) inform the Person from whom Service Provider collects Personal Information:

(i) the purpose for collecting the information,

(ii) the legal authority for collecting the information,

(iii) that Service Provider is collecting the information on behalf of the Province, and

(iv) the title, business address and business telephone number of the Person designated by the Province to answer questions about Service Provider's collection of such Personal Information; and

(c) make every reasonable effort to ensure the accuracy and completeness of Personal Information collected by Service Provider in respect of the Services.

This section does not apply to personal information in respect of Service Provider's Personnel, Access Subcontractor's External Personnel or other the employees of suppliers used in the ordinary course of Service Provider's business except to the extent that the same constitutes Personal Information of such person other than in their role as an employee as contemplated above.

38. Complaints and Investigations

Subject to the provisions of Section 5 *(Directives)* above, in the event of a dispute between either Service Provider and an individual or the Province and an individual, or an investigation or other proceeding before a Privacy Commissioner or other institution or authority, concerning the collection, use, disclosure, or otherwise in respect of Personal Information, Service Provider, will upon the request of the Province defend and advocate the lawfulness of its Personal Information handling practices and its policies and procedures and, at the Province's cost and expense, those policies and procedures of the Province, through all available means of dispute resolution as provided for by Applicable Laws, all in cooperation with the Province.

39. Non-Compliance Reports

Service Provider shall, as soon as possible, and in any event within 24 hours, report to the Province through the Governance Process of any known breach of the requirements of these Privacy Obligations, disclosure of Personal Information, potential disclosure of Personal Information or other risk with respect to the disclosure of Personal Information. If for any reason Service Provider does not comply, or anticipates that it will be unable to comply, with a term of these Privacy Obligations in any respect, then Service Provider shall promptly notify the Province of the particulars of such non-compliance or anticipated non-compliance, and the steps that Service Provider proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance. If the Service Provider fails to take steps to address, or prevent recurrence of, the non-compliance or anticipated non-compliance or if such steps proposed by the Service Provider are not adequate to enable the Service Provider to comply with these Privacy Obligations, in the Province's discretion, then such failure shall be a breach of this Agreement and the Province shall have all rights and remedies under this Agreement.

40. FOIPP Act Inspections

Service Provider acknowledges that under the *Freedom of Information and Protection of Privacy Act*, the Commissioner has the power to obtain information and evidence from Persons other than the Province in the course of conducting an investigation or an inquiry under that Act. Accordingly, Service Provider shall provide reasonable cooperation to the Province with respect to investigations or inquiries of the Commissioner under the *Freedom of Information and Protection of Privacy Act* in connection with any information related to the Agreement that the Commissioner is entitled to obtain under such Act

41. Prohibition Against Foreign Affiliates

Service Provider shall, and shall cause its Access Subcontractors to, prohibit or otherwise restrict, their foreign Affiliates from accessing any Province Information and require that such Personal Information is at all times in the custody of a Canadian Entity, except as may be expressly permitted otherwise under the terms of the Agreement or these Privacy Obligations.

42. Service Provider Directors

Service Provider shall require that throughout the Term its directors shall all be Canadian citizens and residents and in each case who are not US Personnel. All directors of Service Provider shall enter into Confidentiality Covenants or External Confidentiality Covenants, as applicable, with the Province.

43. Indemnification and Limitation of Liability

Any Claims, disputes, procedures or otherwise arising out of this Schedule or the Parties' requirements under the Privacy Obligations, or the disclosure of Personal Information, shall be governed by the provisions Article 25 (*Indemnification, Liability and Guarantees*) of the Agreement and **Schedule 30** (*Indemnification Matters*) and **Schedule 31** (*Limitation of Liability*) of the Agreement.

44. Changes

Any changes, amendments, updates, modifications, revisions, replacements or supplements in or to the Privacy Obligations including:

(a) the form of the Confidentiality Covenant or the External Confidentiality Covenant;

(b) information security management codes of practice, as outlined in ISO27002 (as amended from time to time); or

(c) the security policies, standards, guidelines and practices of the Province as outlined in the Province's Core Policy Manual (http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm) and the Information Technology Security Policy (ISP) (http://www.cio.gov.bc.ca/services/security/ISP.asp);

and Impacting Service Provider's responsibilities under the Agreement will be implemented in accordance with the Change Order Process.

45. Transition

Notwithstanding the provisions of this **Schedule 24** (*Privacy Obligations*), the Service Provider will perform the Services in the same manner that the Province performed such services immediately prior to

the Hand-Over Date with respect to the following provisions, until the times or periods referred to below (each, a "**Privacy Transition Period**"):

(a) Section 17(a) and (b), from and after the Hand-Over Date until the transition of the Services into an STMS Data Centre;

(b) Section 17(e), from and after the Hand-Over Date for networks controlled by the Province and used by the Service Provider to deliver the Services to the Province from the Province Data Centres, the Remote Infrastructure Server Locations and the Remote Application Server Locations, as set forth in **Schedule 8 (Service Locations)**;

(c) Section 17(i), from and after the Hand-Over Date and for a period of six (6) months expiring on October 31, 2009;

(d) Section 18(a) and (b), from and after the Hand-Over Date until the transition of the Services into an STMS Data Centre, the Service Provider will comply with Province Policies, as contemplated in the Data Centre Services SOW;

(e) Section 19(a), from and after the Hand-Over Date and for a period of three (3) months expiring on June 30, 2009;

(f) Section 19(d)(iii), from and after the Hand-Over Date and for a period of three (3) months expiring on June 30, 2009;

(g) Section 19(h), with respect to Province owned equipment and until such Province owned equipment is replaced with Service Provider provided equipment;

(h) Section 25(a), from and after the Hand-Over Date the Systems Logs will be provided by the Service Provider to the Province using the Province's software tools and processes until the transition of the Services into an STMS Data Centre;

For greater clarification, the Service Provider shall perform the Services described above in accordance with the requirements of **Schedule 24** (*Privacy Obligations*) no later than the expiry of the applicable Privacy Transition Period therefore.

From and after the Hand-Over Date, with respect to the Province Data Centres, the Remote Infrastructure Server Locations and the Remote Application Server Locations, the Parties acknowledge that they shall each have Custody of the Personal Information for the period that such Personal Information is located at any of the Province Data Centres, the Remote Infrastructure Server Locations and the Remote Application Server Locations. The Service Provider will have Custody of the Personal Information located at any of the Service Locations set forth in Schedule 8 (*Service Locations*) other than the Province Data Centres, the Remote Infrastructure Server Locations and the Remote Application Server Locations.

With respect to Section 13(a) above, the Service Provider shall not be required to conduct a security threat and risk assessment at the Province Data Centres, the Remote Infrastructure Server Locations and the Remote Application Server Locations, as set forth in **Schedule 8 (Service Locations)**, prior to the provision of Services to the Province from those locations on the Hand-Over Date.

Appendix A – Privacy Protection Schedule

Definitions

1. In this Schedule,

"access" means disclosure by the provision of access;

"Act" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;

"contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

"personal information" means recorded information about an identifiable individual, other than contact information, collected or created by the Service Provider as a result of the Agreement or any previous agreement between the Province and the Service Provider dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the "control of a public body" within the meaning of the Act.

Purpose

2. The purpose of this Schedule is to:

enable the Province to comply with its statutory obligations under the Act with respect to personal information; and

ensure that, as a service provider, the Service Provider is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider may only collect or create personal information that is necessary for the performance of the Service Provider's obligations, or the exercise of the Service Provider's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider must tell an individual from whom the Service Provider collects personal information:

(a) the purpose for collecting it;

(b) the legal authority for collecting it; and

(c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Service Provider's collection of personal information.

Accuracy of personal information

6. The Service Provider must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Service Provider or the Province to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Service Provider receives a request for access to personal information from a person other than the Province, the Service Provider must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Service Provider to provide such access and, if the Province has advised the Service Provider of the name or title and contact information of an official of the Province to whom such requests are to be made, the Service Provider must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Province to correct or annotate any personal information, the Service Provider must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Province must advise the Service Provider of the date the correction request to which the direction relates was received by the Province in order that the Service Provider may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Service Provider must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Service Provider disclosed the information being corrected or annotated.

If the Service Provider receives a request for correction of personal information from a person other than the Province, the Service Provider must promptly advise the person to make the request to the Province and, if the Province has advised the Service Provider of the name or title and contact information of an official of the Province to whom such requests are to be made, the Service Provider must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Service Provider must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Province otherwise directs in writing, the Service Provider must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Service Provider must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Province otherwise directs in writing, the Service Provider may only use personal information if that use is for the performance of the Service Provider's obligations, or the exercise of the Service Provider's rights, under the Agreement.

Disclosure of personal information

16. Unless the Province otherwise directs in writing, the Service Provider may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of the Service Provider's obligations, or the exercise of the Service Provider's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

18. In addition to any obligation the Service Provider may have to provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in its custody or under its control the Service Provider:

receives a foreign demand for disclosure;

receives a request to disclose, produce or provide access that the Service Provider knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or

has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

the Service Provider must immediately notify the Province and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

19. In addition to any obligation the Service Provider may have to provide the notification contemplated by section 30.5 of the Act, if the Service Provider knows that there has been an unauthorized disclosure of personal information in its custody or under its control, the Service Provider must immediately notify the Province. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

20. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Service Provider, enter on the Service Provider' s premises to inspect any personal information in the possession of the Service Provider or any of the Service Provider's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Service Provider must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

21. The Service Provider must in relation to personal information comply with:

(a) the requirements of the Act applicable to the Service Provider as a service provider, including any applicable order of the commissioner under the Act; and

(b) any direction given by the Province under this Schedule.

22. The Service Provider acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

23. If for any reason the Service Provider does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Service Provider must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

24. Rights of termination under this Privacy Protection Schedule are as set out in the Agreementt.

Interpretation

25. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

26. Any reference to the "Service Provider" in this Schedule includes any subcontractor or agent retained by the Service Provider to perform obligations under the Agreement and the Service Provider must ensure that any such subcontractors and agents comply with this Schedule.

27. The obligations of the Service Provider in this Schedule will survive the termination of the Agreement.

28. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

29. The Service Provider must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 30, the law of any jurisdiction outside Canada.

29. The Service Provider must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 30, the law of any jurisdiction outside Canada.

30. Nothing in this Schedule requires the Service Provider to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

Appendix B – Privacy Management Plan

(See attached)

APPENDIX B
TO SCHEDULE 24 (PRIVACY OBLIGATIONS)

Privacy Management Plan

1. **Purpose:** The purpose of the Service Provider Privacy Management Plan is to set out the plan of the Service Provider to address issues related to Privacy in connection with the STMS Project. The Plan encompasses

   (i) the steps to be taken by the Service Provider to implement plans, policies and procedures specific to the Service Provider's privacy and security obligations under the Agreement; and

   (ii) ongoing reviews and updates of the Service Provider' plans, policies and procedures.

2. **Scope**: The Service Provider shall develop and maintain plans, policies and procedures specific to the privacy and security obligations under the Agreement. The Service Provider shall document a Privacy Management Plan that will encompass plans, policies and procedures related to the following:

- **SECURITY POLICY**
  Information security policy document
  Review of the information security policy
- **ORGANIZATION OF INFORMATION SECURITY**
  INTERNAL ORGANIZATION
    - Management commitment to information security
    - Allocation of information security responsibilities
    - Authorization process for information processing facilities
    - Confidentiality agreements

  EXTERNAL PARTIES
    - Identification of risks related to external parties
    - Addressing security in third party agreements
- **ASSET MANAGEMENT**
  RESPONSIBILITY FOR ASSETS
    - Inventory of assets
    - Acceptable use of assets

  INFORMATION CLASSIFICATION
- **HUMAN RESOURCES SECURITY**
  PRIOR TO EMPLOYMENT
    - Introduction to Security
    - Annual Service Provider Personnel Privacy & Security Training
    - Whistleblower Protection
    - Roles and Responsibilities
    - Screening
    - Terms and conditions of employment

  DURING EMPLOYMENT
    - Management responsibilities
    - Information security awareness, education, and training
    - Disciplinary process

TERMINATION OR CHANGE OF EMPLOYMENT
- Termination responsibilities
- Return of assets
- Removal of access rights

- **PHYSICAL AND ENVIRONMENTAL SECURITY**

SECURE AREAS
- Physical security perimeter
- Physical entry controls

EQUIPMENT SECURITY
- Security of equipment off-premises
- Secure disposal or re-use of equipment

- **COMMUNICATIONS AND OPERATIONS MANAGEMENT**

OPERATIONAL PROCEDURES AND RESPONSIBILITIES
- Documented operating procedures
- Change management
- Segregation of duties
- Separation of development, test, and operational facilities

PROTECTION AGAINST MALICIOUS AND MOBILE CODE
- Controls against malicious code
- Controls against mobile code

NETWORK SECURITY MANAGEMENT
- Network controls
- Security of network services

MEDIA HANDLING
- Management of removable media
- Disposal of media
- Information handling procedures
- Security of system documentation

MONITORING
- Audit logging
- Monitoring system use
- Protection of log information
- Administrator and operator logs

- **ACCESS CONTROL**

BUSINESS REQUIREMENT FOR ACCESS CONTROL
- Access control policy

USER ACCESS MANAGEMENT
- User registration
- Privilege management
- User password management
- Review of user access rights

USER RESPONSIBILITIES
- Password use
- Clear desk and clear screen policy

NETWORK ACCESS CONTROL
- Policy on use of network services
- User authentication for external connections
- Remote diagnostic and configuration port protection
- Network connection control
- Network routing control

OPERATING SYSTEM ACCESS CONTROL
- Secure log-on procedures
- User identification and authentication
- Password management system

MOBILE COMPUTING AND TELEWORKING
- Mobile computing and communications
- Teleworking

- **INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE**

SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

CORRECT PROCESSING IN APPLICATIONS

CRYPTOGRAPHIC CONTROLS
- Policy on the use of cryptographic controls
- Key management

TECHNICAL VULNERABILITY MANAGEMENT

- **INFORMATION SECURITY INCIDENT MANAGEMENT**

REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES
- Reporting information security events
- Reporting security weaknesses

MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS
- Responsibilities and procedures
- Learning from information security incidents
- Collection of evidence

- **COMPLIANCE**

CONTRACT COMPLIANCE
- Threat and Risk Assessments
- Privacy Impact Assessments
- Ownership and Control of Personal Information
- US Personnel Restrictions
- Compliance Certificates
- Privacy Impact Assessments
- Security Threat Risk Assessments

COMPLIANCE WITH LEGAL REQUIREMENTS
- Identification of applicable legislation
- Intellectual property rights (IPR)
- Protection of organizational records
- Data protection and privacy of personal information
- Prevention of misuse of information processing facilities
- Regulation of cryptographic controls

COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE
- Compliance with security policies and standards
- Technical compliance checking

INFORMATION SYSTEMS AUDIT CONSIDERATIONS
- Information systems audit controls
- Protection of information systems audit tools

3. **Development and Implementation of Privacy Management Plan**: The Service Provider has well-established policies, standards, processes and procedures covering all

security categories identified in section 2 of this Privacy Management Plan. The transferring services have established processes and procedures that will continue to be utilized until transformed. The existing policies, standards, processes and procedures will be reviewed, adjusted as required, and implemented to accommodate the Services and the specific requirements of the Province. The initial Privacy Management Plan will be completed prior to the first anniversary of the Effective Date of the Agreement.

4. **Timing**. The Service Provider will develop a detailed implementation plan following the Effective Date that will prioritize the plan elements to ensure the critical components required early in the first Contract Year are developed first with all elements to be completed by the end of the fist Contract Year.

5. **Annual Updates**. The Service Provider will update the Privacy Management Plan on an annual basis with completion prior to the anniversary of Effective Date. Processes and Procedures will be updated on an ongoing basis to address operational security requirements and reflect the improvements introduced by the specific Transition and Transformation activities as described in their respective Statements of Work under the Agreement.

6. **Inspection by Province**. Once developed, all components of the Privacy Management Plan will be available for review by the Province on an annual basis. The Service Provider shall make the policies and procedures implemented by it under the Privacy Management Plan available for review by the Province at the Service Provider's premises on an annual basis and at the Province's request. The Service Provider shall advise the Province through the Governance Process defined in the Agreement of any material changes that it has made to such policies and procedures.

7. **Defined Terms**. In this Privacy Management Plan, "Agreement" means the Master Services Agreement dated March 30, 2009 between the Her Majesty the Queen in right of the Province of British Columbia as represented by the Minster of Labour and Citizens' Services and the Service Provider. (Other capitalized terms used without definition (other than in Section 2) have the meaning attached to such terms in the Agreement.)

Appendix C – Confidentiality Covenant

CONFIDENTIALITY COVENANT

BACKGROUND:

Pursuant to a contract to be entered into by the **PROVINCE OF BRITISH COLUMBIA, AS REPRESENTED BY THE MINISTER OF LABOUR AND CITIZENS' SERVICES** (the "**Province**") and **EDS ADVANCED SOLUTIONS INC.** (the "**Company**") for the Strategic Transformation and Mainframe Services Project (the "**Contract**"), EAS will be providing services to the Province and to the Broader Public Sector (or BPS) as defined below. In providing services to the Province and BPS, the Company will be provided with access to or custody over personal information that is under the control of the Province or the BPS, including highly sensitive personal information, and other confidential information (the "**Province/BPS Data**"), and the Company is obligated to ensure the privacy, confidentiality and security of the Province/BPS Data.

DEFINITIONS:

"**Broader Public Sector**" **or** "**BPS**" means crown corporations or agencies that are owned directly or indirectly by the Province, and all other levels of government within British Columbia including, without limitation, all municipalities, cities, towns, counties or other political jurisdictions of British Columbia, or any agency, board, council, department, authority, tribunal or commission of the Province or of any of the foregoing, and includes universities, colleges, schools, school boards, hospitals and health authorities in British Columbia.

"**Foreign Disclosure Laws**" means any laws, statutes, by-laws, treaty, directive, policy having the force of law, order, judgment, injunction, award, decree or other similar matter of any government, legislature (or similar body), court, governmental department, commission, board, bureau, agency, instrumentality, province, state, territory, association, county, municipality, city, town or other political of governmental jurisdiction, whether not or in the future constituted, outside of Canada, that may require, request, or otherwise demand access, use or disclosure of personal information, whether to intercept or obstruct terrorism, or for any other reason.

COVENANT:

I, the undersigned, acknowledge that upon my employment with the Company it will be a condition of my access to Province/BPS Data that I maintain the confidentiality and security of Province/BPS Data and report any breach or suspected breach of confidentiality or security and any wrongdoing or suspected wrongdoing of which I am aware.

I, the undersigned, covenant that upon my employment with the Company:

1. I will access and deal with Province/BPS Data only in strict accordance with the written policies and processes that have been agreed to between the Company and the Province or BPS, to the extent that the same have been delivered or made available to me, including all Company policies that expressly prohibit any disclosure of Province/BPS Data pursuant to Foreign Disclosure Laws (collectively, the "**Privacy Obligations**").

2. I will not disclose any Province/BPS Data except as clearly permitted or provided for by the Privacy Obligations.

3. In the event that I know or suspect that the Company or any other person or organization has accessed or disclosed or intends to access or disclose any Province/BPS Data in any manner that is not permitted by, or that is inconsistent with, the provisions of the Privacy Obligations (a "**Breach**"), I will:

(a) not take any action to assist the Company or any other person in committing the Breach or that might otherwise permit or provide for the furtherance of the Breach, even if instructed to do so by the Company or by any other person; and

(b) immediately notify the Province of the Breach by calling a hotline (telephone number 250-356-1851) that has been established by the Province as set forth in the Privacy Obligations (the "**Hotline**") and cooperate with the Province by providing all relevant information regarding the details of the Breach.

4. Where I have any questions as to whether a Breach has occurred, I will call the Hotline. I will be deemed to be in compliance with my obligations under this Confidentiality Covenant where I follow any direction that I receive from the Province through the Hotline.

5. I am aware that under the ***Freedom of Information and Protection of Privacy Act*** (British Columbia) ("the FOIPP Act"), there are certain obligations placed on me as an employee of a "service provider" and, in particular, an obligation to provide notice to the Province of any foreign demand for disclosure of personal information.

6. I am aware that the FOIPP Act also provides for "whistle blower" protection for those who report incidents relating to foreign demands for disclosure, which requires, among other things, that an employer not discipline an employee because the employee, acting in good faith and on the basis of reasonable belief, has notified the commissioner under the FOIPP Act of an unauthorized disclosure of personal information or has notified the minister responsible under the FOIPP Act of a foreign demand for disclosure.

7. I acknowledge and agree that my obligations to the Province pursuant to this Confidentiality Covenant take priority over any agreement with or commitment to any other party (including the Company) that is inconsistent with this Confidentiality Covenant.

8. I acknowledge and agree that, if I leave the employ of the Company, I will not disclose to any person any Province/BPS Data nor take with me any Province/BPS Data received during the course of my employment with the Company.

9. I will, on an annual basis or as otherwise requested by the Province or the Company, reconfirm my commitments in respect of the Province/BPS Data.

I acknowledge that, upon my employment with the Company, my failure to comply with the provisions of this Confidentiality Covenant will be cause for and may result in disciplinary action up to and including, where necessary, my dismissal from the Company.

IN WITNESS WHEREOF I have executed this Confidentiality Covenant as of the _____ day of _____, _____.

SIGNED, SEALED and DELIVERED by

_____

[**PRINT NAME**]

_____

_____ [**SIGNATURE**]

[Place Seal here]

Signed in the presence of:

_____

Signature of **Witness**

_____

Print Name of **Witness**

_____

Address of **Witness**

_____

_____

Occupation of **Witness**

Appendix D – External Confidentiality Covenant

EXTERNAL CONFIDENTIALITY COVENANT

BACKGROUND:

Pursuant to a contract to be entered into by the **PROVINCE OF BRITISH COLUMBIA, AS REPRESENTED BY THE MINISTER OF LABOUR AND CITIZENS' SERVICES** (the "**Province**") and **EDS ADVANCED SOLUTIONS INC.** (the "**EAS**") for the Strategic Transformation and Mainframe Services Project (the "**Contract**"), EAS will be providing services to the Province and to the Broader Public Sector (or BPS) as defined below. In providing services to the Province and BPS, EAS will be provided with access to or custody over personal information that is under the control of the Province or the BPS, including highly sensitive personal information, and other confidential information (the "**Province/BPS Data**"), and EAS is obligated to ensure the privacy, confidentiality and security of the Province/BPS Data. I am currently employed by ***[Insert name of subcontractor]*** (the "**Company**") and I have been advised that the Company will provide services to EAS as a subcontractor in connection with the Strategic Transformation and Mainframe Services Project and in providing services to the Province and BPS, the Company will be provided with access to or custody over personal information that is under the control of the Province or the BPS, including Province/BPS Data.

DEFINITIONS:

"**Broader Public Sector**" **or** "**BPS**" means crown corporations or agencies that are owned directly or indirectly by the Province, and all other levels of government within British Columbia including, without limitation, all municipalities, cities, towns, counties or other political jurisdictions of British Columbia, or any agency, board, council, department, authority, tribunal or commission of the Province or of any of the foregoing, and includes universities, colleges, schools, school boards, hospitals and health authorities in British Columbia.

"**Foreign Disclosure Laws**" means any laws, statutes, by-laws, treaty, directive, policy having the force of law, order, judgment, injunction, award, decree or other similar matter of any government, legislature (or similar body), court, governmental department, commission, board, bureau, agency, instrumentality, province, state, territory, association, county, municipality, city, town or other political of governmental jurisdiction, whether not or in the future constituted, outside of Canada, that may require, request, or otherwise demand access, use or disclosure of personal information, whether to intercept or obstruct terrorism, or for any other reason.

COVENANT:

I, the undersigned, acknowledge that upon my employment with the Company it will be a condition of my access to Province/BPS Data that I maintain the confidentiality and security of Province/BPS Data and report any breach or suspected breach of confidentiality or security and any wrongdoing or suspected wrongdoing of which I am aware.

I, the undersigned, covenant that upon my employment with the Company:

1. I will access and deal with Province/BPS Data only in strict accordance with the written policies and processes that have been agreed to between the Company and the Province or BPS, to the extent that the same have been delivered or made available to me, including all Company policies

that expressly prohibit any disclosure of Province/BPS Data pursuant to Foreign Disclosure Laws (collectively, the "**Privacy Obligations**").

2. I will not disclose any Province/BPS Data except as clearly permitted or provided for by the Privacy Obligations.

3. In the event that I know or suspect that the Company or any other person or organization has accessed or disclosed or intends to access or disclose any Province/BPS Data in any manner that is not permitted by, or that is inconsistent with, the provisions of the Privacy Obligations (a "**Breach**"), I will:

   (a) not take any action to assist the Company or any other person in committing the Breach or that might otherwise permit or provide for the furtherance of the Breach, even if instructed to do so by the Company or by any other person; and

   (b) immediately notify the Province of the Breach by calling a hotline (telephone number 250-356-1851) that has been established by the Province as set forth in the Privacy Obligations (the "**Hotline**") and cooperate with the Province by providing all relevant information regarding the details of the Breach.

4. Where I have any questions as to whether a Breach has occurred, I will call the Hotline. I will be deemed to be in compliance with my obligations under this Confidentiality Covenant where I follow any direction that I receive from the Province through the Hotline.

5. I am aware that under the ***Freedom of Information and Protection of Privacy Act*** (British Columbia) ("the FOIPP Act"), there are certain obligations placed on me as an employee of a "service provider" and, in particular, an obligation to provide notice to the Province of any foreign demand for disclosure of personal information.

6. I am aware that the FOIPP Act also provides for "whistle blower" protection for those who report incidents relating to foreign demands for disclosure, which requires, among other things, that an employer not discipline an employee because the employee, acting in good faith and on the basis of reasonable belief, has notified the commissioner under the FOIPP Act of an unauthorized disclosure of personal information or has notified the minister responsible under the FOIPP Act of a foreign demand for disclosure.

7. I acknowledge and agree that my obligations to the Province pursuant to this Confidentiality Covenant take priority over any agreement with or commitment to any other party (including the Company) that is inconsistent with this Confidentiality Covenant.

8. I acknowledge and agree that, if I leave the employ of the Company, I will not disclose to any person any Province/BPS Data nor take with me any Province/BPS Data received during the course of my employment with the Company.

9. I will, on an annual basis or as otherwise requested by the Province or the Company, reconfirm my commitments in respect of the Province/BPS Data.

I acknowledge that, upon my employment with the Company, my failure to comply with the provisions of this Confidentiality Covenant will be cause for and may result in disciplinary action up to and including, where necessary, my dismissal from the Company.

IN WITNESS WHEREOF I have executed this Confidentiality Covenant as of the _____ day of _____, _____.

SIGNED, SEALED and DELIVERED by

_____
[**PRINT NAME**]

_____
[**SIGNATURE**]

[Place Seal here]

Signed in the presence of:

_____
Signature of **Witness**

_____
Print Name of **Witness**

_____
Address of **Witness**

_____

_____
Occupation of **Witness**

SCHEDULE 25

CORPORATE CHART

To be provided on the Effective Date.

SCHEDULE 26

GROWTH AND MARKETING

1. Purpose.

The purpose of this Schedule 26 (*Growth and Marketing*) is to describe the agreement between the Province and the Service Provider regarding the joint efforts of the Parties to market the Services under STMS to Broader Public Sector entities wishing to purchase such Services under STMS.

2. Definitions.

Capitalized words used in this Schedule 26 (*Growth and Marketing*) shall have the meanings given to such words in the Agreement. In the event that a term is not defined in the Agreement, it shall have the meaning provided in this Section 2 of this Schedule or in the body of this Schedule.

"Adjusted Capacity Reservation" has the meaning given to it in Schedule 23 (*Fees*).

"Capacity Reservation" has the meaning given to it in Schedule 23 (*Fees*).

"Potential Buyer" means Broader Public Sector entities interested in purchasing Services under STMS.

"Province Adjusted VA Commitment" has the meaning given to it in Schedule 23 (*Fees*).

"Province VA Commitment" has the meaning given to it in Schedule 23 (*Fees*).

"VA" has the meaning given to it in Schedule 23 (*Fees*).

3. Principles.

3.1 *Hosting Solutions BC.* The Parties acknowledge and agree that they will promote STMS under the brand "Hosting Solutions BC". The Parties will market the Services and STMS in the province of British Columbia, in the public sector market. The Parties agree to adhere to the practices and processes described in this Schedule 26 (*Growth and Marketing*) and as otherwise determined by the Joint Marketing Committee.

3.2 *Marketing to the Broader Public Sector.* The Parties will proactively identify and encourage Broader Public Sector to become either Clients of WTS or Buyers under this Agreement.

3.3 *Public Procurements.* If there is a public procurement issued by a Broader Public Sector entity for services that are similar to the Services under the Agreement, then the Service Provider will immediately notify the Province, through Strategic Infrastructure (with a copy to the members of the JMC), so the Province has an opportunity to discuss with such Broader Public Sector entity the potential benefits and opportunities for such entity under STMS.

It is the desire of the Parties that: (i) if the Service Provider (or the Data Centre Services Subcontractor) is the successful proponent in a public procurement issued by a Broader Public Sector entity for services from an STMS Data Centre similar to the Services, then any VA's associated with such services shall be counted toward the Province VA Commitment or the Province Adjusted VA Commitment, as the case may be, for purposes of determining the VA Unit Price for all Buyers; and (ii) in connection with such

procurement, Service Provider (or the Data Centre Services Subcontractor if applicable) shall not be obligated to use the same pricing or products as contemplated in the Agreement. Following the Effective Date, the Parties will work jointly together to implement the foregoing arrangement in a timely manner that is in accordance with all Applicable Laws.

4. Joint Marketing Committee.

The Parties will establish a Joint Marketing Committee (JMC), as contemplated in Schedule 18 (*Governance*) of the Agreement. The JMC will report to the Joint Executive Committee (JEC) under the Agreement.

4.1 *Scope and Responsibilities of the JMC.* The overall scope and responsibility of the JMC is as follows:

- to the extent possible, ensure that the marketing and onboarding interests of the Parties are aligned;
- develop an annual joint business development plan including goals and targets, and budgets for approval by the JEC;
- establish principles and practices for sharing information about the market and prospects between the Service Provider and the JMC;
- establish, and up-date as appropriate, marketing, sales and onboarding processes including the qualification of prospects, leveraging the Service Provider's (and its Affiliate's) processes;
- establish, and up-date as appropriate, standards for proposals, leveraging Service Provider's (and its Affiliate's) standards;
- monitor progress against tactical marketing and onboarding plans and activities;
- ensure the benefits of gainsharing are applied consistently with the terms of Schedule 27 (*Gainsharing*);
- approve all joint communications and marketing materials to be released by the Parties;
- approve and undertake major marketing events as appropriate;
- escalate to JEC in the event of conflict or dispute;
- prepare annual progress reports on marketing and onboarding activities;
- monitor relationships with key Stakeholders; and
- monitor the reputation of Hosting Solutions BC and its services.

4.2 *Business Development.* The focus of the JMC is the entire portfolio of STMS shared services and the value proposition of the Agreement to Broader Public Sector entities.

4.3 *Branding.* STMS will operate under the name Hosting Solutions BC.

4.4 *Budget and Cost Sharing.* The Province, through Strategic Infrastructure ("**SI**"), and the Service Provider will jointly establish a budget within three months of the start of each Contract Year for the upcoming year for the marketing and business development activities associated with STMS. Each Party will pay for their own costs associated with the marketing and business development activities contemplated under this Schedule 26 (*Growth and Marketing*), unless the Parties agree otherwise to share such any costs. For greater certainty, there will be no flow of funds between the Province and the Service Provider as a reimbursement of the other Party's costs.

4.5 *Documentation.* The Parties will jointly develop the following:

(a) *JMC Annual Plan:* an annual plan in connection with the marketing and business development activities for STMS ("**JMC Annual Plan**"), which shall be the overall guiding document for the JMC. The JMC Annual Plan must take into account feedback from the previous Contract Year on what was successful, and any suggested improvements and changes. The JMC Annual Plan will also incorporate the following key elements:

- *Key goals and targets* based on objectives of the Parties;
- *Budget* for JEC approval;
- *Products and services roadmap* that incorporates any planned changes to the existing service offerings to be introduced during the year;
- *Messaging / value proposition for Services* with sensitivity to any negative market perception of the deal;
- *Reporting requirements* based on key metrics identified. Examples of potential metrics are VAs, unit price reductions, overall revenue, Managed Services growth and Buyer satisfaction.

(b) *JMC Business Development Plan:* a business development plan (the "**JMC Business Development Plan**") will be developed annually and presented by the JMC to the JEC by the end of February each Contract Year in preparation for the upcoming Contract Year. The Province and the Service Provider will jointly develop the plan, with overall accountability for the JMC Business Development Plan to be with the Business Relationship Executive, Strategic Infrastructure. The Parties acknowledge and agree that the ADM SI, WTS, MLCS Integrated Services Solutions Division, and existing Buyers under the Agreement will be part of the consultative process in developing the JMC Business Development Plan. The JMC Business Development Plan will also incorporate the following key elements:

- Outline the onboarding strategy for the next Contract Year;
- Calendar of events covering tradeshows, conferences, and other functions in alignment with the strategy;
- Client profiles, segmentation and respective action plan
- Metrics outlining success criteria;
- Relationship strategies; and
- Types of services to focus on.

(c) *Workshops:* Parties will hold joint workshops in the fourth quarter of the preceding Contract Year in preparation for end of February delivery commitment. The Parties will ensure appropriate personnel, resources and information is made available.

(d) *Materials:* The JMC will create marketing, sales and promotional materials, the development of which will be the overall responsibility of the Business Relationship Executive, Strategic Infrastructure, in collaboration with the Service Provider. The marketing, sales and promotional materials are to support the overall JMC Business Development Plan, the costs of which must be included in the annual budget in the JMC Annual Plan.

(e) *Websites:* There will be an internal website for Buyers and an external website for Potential Buyers. For the internal website, Service Provider will act in a consultative role with respect to the content, acknowledging that some content will be confidential to the Province. The following activities relating to the external website will be carried out by the Parties as indicated below:

- the design of the website will be developed and maintained collaboratively by SI, WTS, and the Service Provider, with SI as the lead;
- development and operating costs for the website will be split equally between the Parties;
- SI and the Service Provider will establish a website budget prior to the beginning of each Contract Year; and
- the Province will be responsible for hosting the website.

(f) *Responsibilities for Creation, Review and Approval of Documentation:* The responsibility for the preparation of the documentation contemplated in this Schedule 26 (*Growth and Marketing*) shall be as set forth in the Table 2 (Development of Documentation) below:

	MLCS Integrated Service Solutions Division	SI		WTS			SP
		BRE	ADM	ED, Client Services	ED, AMO	ADM	
Develop and update the JMC Business Development Plan	I	A, R	C, *	C	C	C	R
Creation of marketing materials (i.e. written sales promotion)	C	A, R	C, *	C	C	C	R

ADM = Assistant Deputy Ministers, Strategic Infrastructure and WorkPlace Technology Services (WTS)
BRE = Business Relationship Executive, SI
ED, AMO = Executive Director, Alliance Management Office WTS
ED, Client Services = Executive Director, Client Services WTS
MLCS = Ministry of Labour and Citizens' Services
SI = Strategic Infrastructure
SP = Service Provider
(R) Responsible: those who are responsible for doing the work
(A) Accountable: those who are accountable for the outcome of the work
(C) Consulted: those who must be consulted to get all relevant facts and information
(I) Informed: Those who must be informed
* = Approval Authority

4.6 *Sales and Onboarding*. Onboarding of new Buyers is an important factor to further increase the value of the shared services model. Through SI, all Buyers of the Services will jointly plan and manage their Capacity Reservation for VAs against the Province VA Commitment or Province Adjusted VA Commitment, as the case may be. As consumption of Services grows over the Term, the Service Provider will be responsible for ensuring that the appropriate volume price discount will be applied to all Buyers. The Province, through SI, will monitor to ensure that the discounts are applied consistent with Schedule 23 (*Fees*). Schedule 23 (*Fees*) sets forth, in detail, the process for each Buyer to increase or reduce their Capacity Reservation.

4.7 *Process*. For all Potential Buyers interested in purchasing Services under STMS, the Parties will follow the process depicted in the attached Appendix A (Potential Buyer – On-boarding Process) of this Schedule 26 (*Growth and Marketing*). The Parties will carry out the following responsibilities:

- SI BRE and EDS Sales Executive will endeavour to align early on in the engagement of a Potential Buyer;

- the Parties will use the Service Provider qualifying criteria to assess the initial opportunity. The Parties acknowledge and agree that it is important to diligently assess the potential early on in the process;

- the Parties acknowledge and agree that the key qualifying activities to validate and qualify the opportunity include:

    - conducting Potential Buyer meetings (frame value hypothesis and dialogue with client, explore issues, elicit context/constraints);

    - gaining access to key stakeholders;

    - assessing our ability to respond;

    - qualifying Potential Buyer resources; and

    - determining Potential Buyer decision and buying process; and

- all opportunities will be documented and tracked in CRM software.

5. Addition of New Buyers.

Upon completion of the process described in Section 4.7 above, SI will work with the Potential Buyer to establish the following:

- the requirements of such Potential Buyer for Services based upon the Services set out in the Services Catalogue for STMS;

- whether such Potential Buyer will purchase Data Centre Services only (co-location services) or Managed Services;

- whether such Potential Buyer will purchase Services through WTS pursuant to an agreement as may be applicable, in which case such Potential Buyer will not have a stand alone BPS Services Agreement directly with the Service Provider and WTS will manage the Services with the Service Provider on the Potential Buyer's behalf;

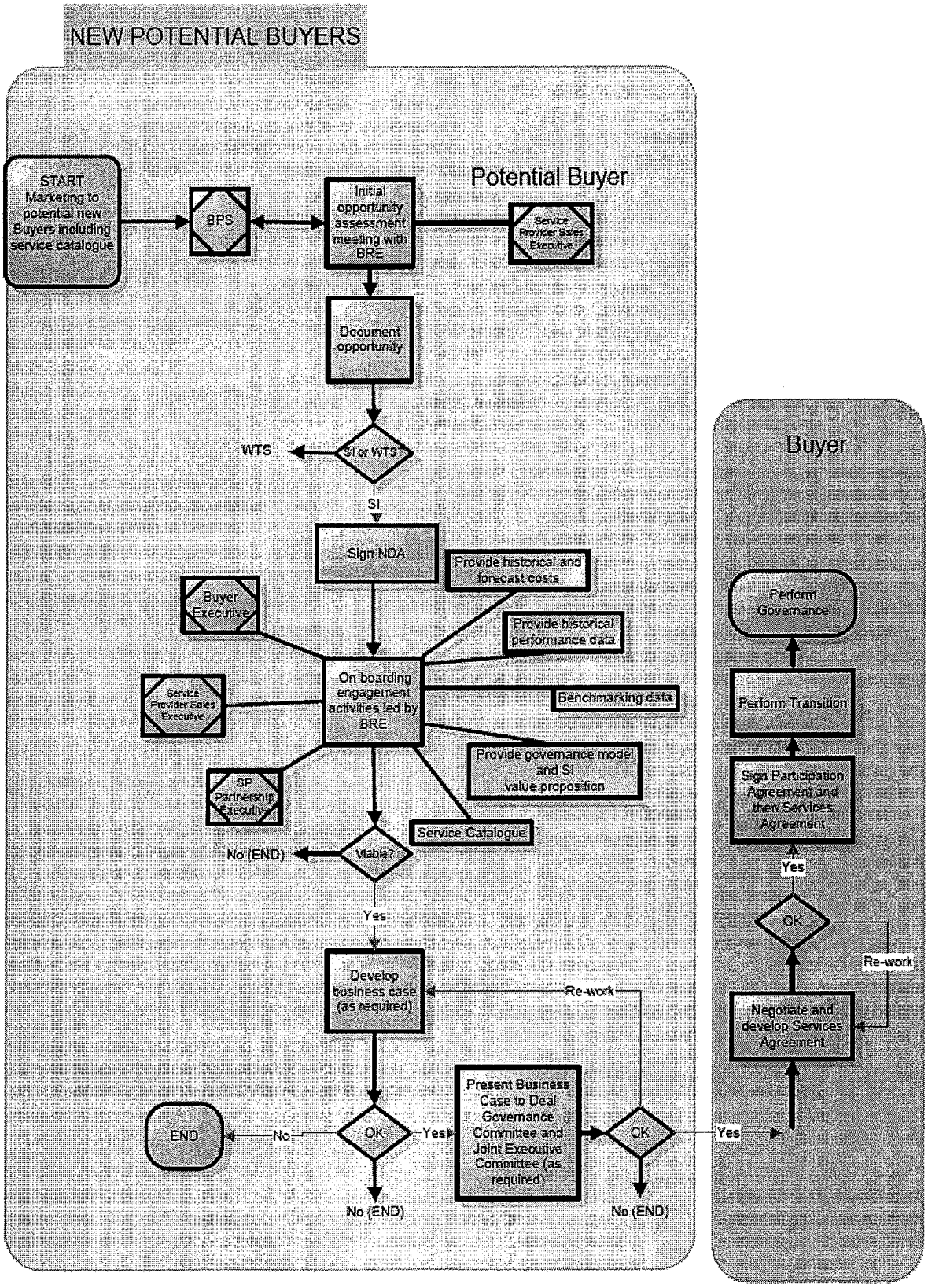
- whether such Potential Buyer will purchase Services directly from the Service Provider, in which case, the Potential Buyer must enter into: (1) a BPS Services Agreement with the Service Provider (which agreement shall be in the same or substantially similar form as the BPS Services Template attached as Appendix B (BPS Services Agreement Template) to this Schedule 26 (*Growth and Marketing*); and (2) Participation Agreement among the Province and other Broader Public Sector entities purchasing Services under STMS;

- whether such Potential Buyer has any special requirements that must be accommodated; and

- the scope of due diligence required by such Potential Buyer and such other information as may be relevant to such Potential Buyer.

APPENDIX A

POTENTIAL BUYER ON-BOARDING PROCESS



APPENDIX B

BPS SERVICES AGREEMENT TEMPLATE

(See attached)

BPS SERVICES AGREEMENT TEMPLATE

between

[INSERT BPS ENTITY]

and

EDS ADVANCED SOLUTIONS INC.

as of March •, 2009

BPS SERVICES AGREEMENT TEMPLATE

TABLE OF CONTENTS

ARTICLE 1 – INTERPRETATION AND GENERAL MATTERS

1.1 Definitions.

Unless otherwise provided in this Agreement (or in any Schedules attached to this Agreement), capitalized terms will have the meanings given to those terms in the attached **Schedule 1** *(Definitions)*. In addition to the definitions contained in **Schedule 1** *(Definitions)*, any capitalized terms defined elsewhere in this Agreement will have the meanings so given to them.

1.2 Recitals.

The recitals to this Agreement are intended to be a general introduction to this Agreement and are not intended to expand the scope of the Parties' obligations under this Agreement or to alter the plain meaning of the terms and conditions of this Agreement.

1.3 Headings.

The division of this Agreement into Articles, Sections, Subsections, paragraphs and clauses, and the insertion of headings, are for convenience of reference only and will not affect the construction or interpretation of this Agreement.

1.4 Interpretation.

In this Agreement, unless expressly stated to the contrary:

(a) the terms "this Agreement", "hereof", "hereunder", "hereto" and similar expressions refer, unless otherwise specified, to this Agreement taken as a whole and not to any particular Article, Section, Subsection, paragraph, clause or other portion of this Agreement;

(b) words importing the singular number only will include the plural, and vice versa, and words importing gender will include all genders;

(c) unless something in the subject matter or context is inconsistent therewith, all references in this Agreement to Articles, Sections, Subsections, paragraphs, clauses and Schedules refer to Articles, Sections, Subsections, paragraphs, clauses and Schedules of this Agreement;

(d) words and phrases denoting inclusiveness (such as "including" or "includes"), whether or not stated as being without limitation, are not limited by their context or the words or phrases which precede or succeed them;

(e) unless otherwise provided in this Agreement, whenever the words "discretion", "option", "determine", "election" and other similar words or any variations thereof are used with respect to a Party, they will be deemed to mean such Party's sole and absolute discretion, option, determination, election or other such similar act;

(f) any reference to a statute will be deemed to refer to the statute and any regulations made thereunder in force as at the date hereof, as the same may be subsequently amended,

expanded, added-to, supplemented or otherwise changed or replaced from time to time, unless otherwise expressly provided in this Agreement; and

(g) unless specifically provided otherwise in this Agreement, any reference to "knowledge" of the Service Provider or any officer or other personnel of the Service Provider means the knowledge of the Service Provider after having made due enquiry, and if the Service Provider fails to make such due enquiry, then the knowledge that the Service Provider would have had if the Service Provider had conducted reasonable enquiry into the subject matter.

1.5 Acting Reasonably.

With respect to the Service Provider, any requirement set forth in this Agreement for the Service Provider to act reasonably, use reasonable efforts, or any variations thereof, will mean the use of all reasonable commercial efforts having regard to the surrounding circumstances, unless specifically provided otherwise. With respect to the Province, any requirement set forth in this Agreement for the Province to act reasonably, use reasonable efforts, or any variations thereof (including, without limitation, any requirement for Approvals by the Province not to be unreasonably withheld), will not require the Province to act in a manner that is contrary to, or is inconsistent with, any other policies, directives, executive directions, Treasury Board decisions, guidelines, rules, regulations, legislation or other determinations of the Province. In addition, the Service Provider expressly acknowledges and confirms that nothing contained in this Agreement will be construed or otherwise interpreted in any manner that would or could cause the Province to fetter its discretion.

1.6 Accounting Policy.

In this Agreement all references to "**GAAP**" refer, unless otherwise specified, to generally accepted accounting principles from time to time approved by the Canadian Institute of Chartered Accountants (or any applicable successor institute thereto) as at the date on which such calculation is made or required to be made, consistently applied. Unless otherwise provided in this Agreement, all accounting, record keeping, book keeping and other actions of the Service Provider contemplated in this Agreement will be performed and carried out in a manner that is consistent with GAAP.

1.7 Calculation of Time Periods.

Unless otherwise specified in this Agreement, when calculating the period of time within or following which any act is to be done or any step taken, the date that is the reference date for starting the calculation of such period will be excluded and the final date for completing such act or step will be included.

1.8 Currency References.

Unless otherwise specified, all dollar references in this Agreement are deemed to refer to lawful money of Canada.

1.9 Time.

Time will be of the essence of this Agreement.

1.10 Schedules.

The following are the Schedules attached to this Agreement, which are incorporated into this Agreement by reference and are deemed to be an integral part of this Agreement: **[NOTE – Schedules to be added, deleted and otherwise adjusted as required.]**

Schedule 1 - Definitions
Schedule 2 - Transition Plan
Schedule 3 - Transition Management and Governance
Schedule 4 - Work-in-Progress Projects
Schedule 5 - Special Terms
Schedule 6 - Basic Services
Schedule 7 - Language of Services
Schedule 8 - Service Locations
Schedule 9 - Transformation
Schedule 10 - Transformation Plan
Schedule 11 - Service Levels
Schedule 12 - Service Level Failures
Schedule 13 - Changes to Weightings
Schedule 14 - Non-Disclosure Agreement
Schedule 15 - Conditions of Use of Province Marks
Schedule 16 - Province Marks
Schedule 17 - Communications Plan and Processes
Schedule 18 - Governance
Schedule 19 - Key Positions
Schedule 20 - Subcontractor Matters
Schedule 21 - Reporting Requirements
Schedule 22 - Records Protocols
Schedule 23 - Fees
Schedule 24 - Privacy Obligations
Schedule 25 - Corporate Chart
Schedule 26 - Growth and Marketing
Schedule 27 - Gainsharing
Schedule 28 - Specific Laws and Policies
Schedule 29 - Additional Representations and Warranties
Schedule 30 - Indemnification Matters
Schedule 31 - Limitation on Liability
Schedule 33 - Financial Guarantee
Schedule 33 - Financial Guarantee
Schedule 34 - Insurance
Schedule 35 - Form of Insurance Certificate
Schedule 36 - Material Breach
Schedule 37 - Remedies for Material Breach
Schedule 38 - Termination Fees
Schedule 39 - Service Provider Code of Conduct
Schedule 40 - JSRFP
Schedule 41 - Province Shared Infrastructure

1.11 Document Conflicts.

The main body of this Agreement, the Schedules attached to this Agreement, the Transaction Documents and the JSD Agreement are to be interpreted so that all of the provisions are given as full effect as

possible. In the event of a conflict among the foregoing, and unless expressly stated to the contrary, the order of precedence will be as follows:

(a) first, the main body of this Agreement;

(b) second, any Schedules attached to this Agreement;

(c) third, any other Transaction Documents; and

(d) fourth, the JSD Agreement.

1.12 Joint Drafting.

The Parties have jointly contributed to the drafting of this Agreement, the Schedules attached to this Agreement and the Transaction Documents. Accordingly, it is the intention of the Parties that the principle of *contra proferentem* will not apply with respect to interpretation matters in respect of this Agreement or the other Transaction Documents.

1.13 Objectives of the Parties.

The Parties acknowledge and agree that the primary objectives and guiding principles of their contractual relationship under this Agreement are as follows:

(a) for the Service Provider to transition and deliver certain **[insert high level description of the services]**, as well as other additional services set forth in or contemplated by this Agreement;

(b) **[insert Province's objectives]**;

(c) to develop a long term and mutually beneficial business relationship characterized by, among other things, mutual cooperation, good faith and flexibility to allow for the addition or removal of services within the scope of the Services described in (and in accordance with) this Agreement, as well as the flexibility to make such adjustment to the Services as may be necessary or otherwise required as a result of any unforeseen conditions or circumstances;

(d) to allow the Service Provider to meet or exceed the Province's service delivery requirements and service levels as described in this Agreement with respect to the Services, and where possible, to continually seek improvement in the delivery of all aspects of the Services;

(e) to develop sufficient business processes to accommodate volume fluctuations inherent in the nature of the Services being delivered;

(f) to have the Service Provider act as a source of "best practices" for the Province by having the Service Provider (and its Affiliates) monitor and evaluate changes and trends in the **[insert high level description of Service industry]** field (including an evaluation of related available and emerging technologies and services), and to so inform the Province in respect thereof from time to time;

(g) to protect the security and privacy of the Personal Information of the Province so that there is no material risk that any such information:

(i) will be disclosed or used contrary to the terms of this Agreement or any Applicable Laws, or

(ii) exists, is stored or can otherwise be accessed anywhere other than in British Columbia (or elsewhere in Canada as may be permitted under or pursuant to this Agreement), whether in its original form or otherwise, without the Approval of the Province;

(h) to minimize any adverse impact on the applicable personnel and business operations of the Province by effectively structuring and managing the transition of the responsibility for the delivery of the Services to the Service Provider;

(i) **[insert additional objectives as appropriate]**; and

(j) to provide for the transition of the Services (other than the Termination Services) to the Province or the Alternative Service Provider upon the expiry or earlier termination of this Agreement in a manner that is efficient, enables continued and uninterrupted delivery of such Services during each such transition, and minimizes any adverse impact on the businesses of the Province in connection therewith.

The Parties acknowledge and agree that the above noted objectives and guiding principles are not, as such, intended to create legal obligations for the Parties, but instead, are intended to document the mutual primary objectives of the Parties in entering into this Agreement. The specific provisions of this Agreement and the other Transaction Documents are to be interpreted according to their plain meaning; provided that where there is uncertainty concerning the meaning of any specific provision, then such provision is to be interpreted in light of the objectives and guiding principles set forth in this Section.

1.14 General Scope.

The potential scope of the Services for the Term of this Agreement is as follows, subject to the implementation of such Services at the discretion of the Province in accordance with the Change Order Process and other applicable terms of this Agreement:

(a) the Services described as being in-scope for this Agreement in the provisions of this Agreement (and any Schedules attached to this Agreement); and

(b) the scope of the services set forth in the JSRFP including, without limitation, any potential scope, future scope or other similarly described scope in the JSRFP.

The Parties acknowledge that it is their intention to expand the Services throughout the Term within the potential scope of Services for this Agreement, as set forth above. Notwithstanding the foregoing, the Service Provider acknowledges and agrees that any additional services that are within such potential scope are subject to negotiation (to the extent applicable) and incorporation into this Agreement through the Change Order Process, by a written instrument signed by the Parties, or as may otherwise be specifically provided for under the terms of this Agreement. The reference to such potential scope in this Section or elsewhere in this Agreement does not, in and of itself, give the Service Provider any automatic or implied right to negotiate, discuss, or incorporate any additional services under this Agreement within such potential scope, and such negotiations, discussions or incorporation will be at the sole discretion of the Province.

ARTICLE 2 – AGREEMENT TERM AND RENEWAL

2.1 Initial Term.

The "**Initial Term**" of this Agreement will commence on the date of this Agreement and will continue until the earlier of:

(a) the date upon which this Agreement is terminated in accordance with the provisions of this Agreement; or

(b) **[insert date]**, as may be extended in accordance with Section 2.7 (*One Year Extension*).

2.2 No Renewal Assurances.

The Province is giving no assurances whatsoever to the Service Provider, expressed or implied, that this Agreement will be renewed or extended beyond the expiry of the Initial Term. The Service Provider specifically acknowledges and affirms that it has arranged its business affairs on the assumption that this Agreement may terminate, at the latest, at the end of the Initial Term.

2.3 No Expropriation.

Any termination of this Agreement in accordance with its terms, either at the expiry of the Initial Term or as otherwise provided in this Agreement, will not constitute an expropriation by the Province or be tantamount to an expropriation by the Province at domestic or international law (including, but not limited to the *North American Free Trade Agreement*), and will not constitute grounds for asserting any Claim whatsoever under any domestic law, international agreement, or domestic law implementing an international agreement (including, but not limited to, Chapter Eleven of the *North American Free Trade Agreement* and the *General Agreement on Trade in Services*).

2.4 Renewal Option.

The Province, at its sole option and acting in its discretion, may elect to renew the Initial Term of this Agreement for one (1) additional renewal term of **[insert number of years for the renewal period]** years expiring on **[insert expiry date for the renewal period]**, or if the Initial Term is extended pursuant to Section 2.7 (*One Year Extension*), then such date that expires **[insert number of years for the renewal period]** years thereafter (the "**Renewal Term**"). The Province may elect to renew this Agreement for the Renewal Term by delivering written notice of such renewal to the Service Provider in accordance with the provisions of Section 2.5 (*Renewal Notice*), but subject to the provisions of Section 2.6 (*Renewal Negotiations*). No such renewal of the Initial Term will prevent either Party from exercising its rights to terminate this Agreement in accordance with its terms.

2.5 Renewal Notice.

Where the Province intends to renew the Initial Term, it will provide the Service Provider with prior written notice of its intent to renew the Initial Term on or before **[insert date]**. If the Province does not deliver such notice to the Service Provider on or before such date, then the Province will be deemed to have elected not to renew the Initial Term of this Agreement.

2.6 Renewal Negotiations.

The terms and conditions of this Agreement will apply during the Renewal Term except for the following, which will be subject to renegotiation and agreement by the Parties acting in good faith (which renegotiations will commence following receipt of a renewal notice by the Service Provider):

(a) in the case of a complete renewal of all of the Services (which renewal will only be effective if the Parties are able to agree upon all of the terms thereof within the time required pursuant to this Section):

(i) **[insert a high level description of the limited provisions that are eligible for renegotiation upon renewal, such as service levels, fees, etc.]**, and

(ii) such provisions of this Agreement which may require consequential amendments as a result of the foregoing; or

(b) in the case of a partial renewal of some but not all of the Services (which partial renewal will only be effective if the Parties are able to agree upon all of the terms thereof within the time required pursuant to this Section):

(i) the part of the Services under this Agreement to be performed by the Service Provider during the Renewal Term (and for greater clarification, the determination and negotiation thereof will be for purposes of identifying such partial Services, and not for purposes of creating new partial Services that are not otherwise included in the Services then performed by the Service Provider prior to the Renewal Term),

(ii) **[insert a high level description of the limited provisions that are eligible for negotiation in connection with the partial services, such as service levels, fees, etc.]** as they relate to the partial Services to be performed during the Renewal Term, and

(iii) such provisions of this Agreement which may require consequential amendments as a result of the foregoing.

If the Parties are able to successfully conclude an agreement upon the foregoing within **[insert number of days permitted for the renewal discussions]**, then they will execute a renewal agreement (the "**Renewal Agreement**") on or before the expiry of such period setting forth the negotiated terms that will apply to the Renewal Term, which terms will be effective from and after **[insert date]**, being the first calendar day following the expiry of the Initial Term (as such date may be extended pursuant to Section 2.7 (*One Year Extension*)), or such other date as may be agreed to in writing by the Parties. If the Parties fail to agree upon the foregoing terms and fail to execute the Renewal Agreement on or before **[insert date]**, or such other date as may be agreed to in writing by the Parties, then there will be deemed to be no Renewal Term for this Agreement (whether for a partial renewal or a full renewal of the Services), and subject to Section 2.7 (*One Year Extension*), the Term will expire at the end of the Initial Term or earlier in accordance with the terms of this Agreement.

2.7 One Year Extension.

The Province, at its sole option and acting in its discretion, may elect to extend the Initial Term (unless the Parties have entered into a Renewal Agreement, in which case, the Province may elect to extend the Renewal Term), for one (1) additional twelve (12) month period (the "**Extension**"), by delivering written

notice of such extension to the Service Provider in accordance with the provisions of Section 2.8 (*Extension Notice*). The Parties acknowledge that the purpose for granting the Province the option to extend the Initial Term, or the Renewal Term, as the case may be, is to allow the Province to conclude any procurement or other related process that it may undertake in connection with the selection of a new service provider for the Services or the repatriation of the Services in-house with the Province, as the case may be.

2.8 Extension Notice.

Where the Province intends to extend the Initial Term (or the Renewal Term, as the case may be), it will provide the Service Provider with prior written notice of its election to extend as follows:

(a) in the case of the Initial Term, on or before **[insert date]**; or

(b) in the case of the Renewal Term, on or before **[insert date]**.

If the Province does not deliver such notice to the Service Provider within the time required, then the Province will be deemed to have elected not to extend the Initial Term or the Renewal Term, as the case may be.

2.9 Extension Terms.

Unless otherwise agreed to in writing by the Parties, the terms and conditions in effect as at the end of the Initial Term or the Renewal Term, as the case may be, being the terms and conditions set forth in this Agreement as amended, changed, modified or supplemented by the Parties in the manner contemplated under this Agreement, will apply during such Extension.

2.10 Termination Assistance.

In connection with the expiry or earlier termination of this Agreement, the Service Provider will provide the Termination Services to the Province in accordance with Article 29 (*Termination Services*).

2.11 Effect of Termination.

The expiry or earlier termination of this Agreement will cause, and will be deemed to cause, the expiry or earlier termination of all other Transaction Documents as of the same date, except for those provisions in this Agreement and in the other Transaction Documents, which are stated to survive Termination.

ARTICLE 3 – INITIAL TRANSITION

3.1 Master Transfer Agreement.

Each Party will perform its respective obligations as set out in the Master Transfer Agreement in accordance with its terms.

3.2 Hand-Over of Services.

Subject to the provisions of this Article 3 (*Initial Transition*), the Parties will transfer responsibility and accountability for the provision of the Services to the Service Provider (the "**Transition**"), with effect on the Hand-Over Date. In connection therewith, the Service Provider will commence the delivery of the Services on the Hand-Over Date, other than those Services that are expressed in this Agreement as being

Services that are to be commenced by the Service Provider on some date other than the Hand-Over Date (such as the Transition Services and the Termination Services).

3.3 Transition Services.

For purposes of completing the Transition, and from and after the execution of this Agreement, the Service Provider will provide the following services to the Province (collectively, the "**Transition Services**"):

(a) such services as are necessary to complete the Transition by the Hand-Over Date and in a manner that will, to the greatest extent possible, ensure the continued, uninterrupted and efficient delivery of the Services throughout the transition, and that will minimize any disruption to the business operations of the Province;

(b) the complete and timely performance by the Service Provider of all matters required to be performed by or on behalf of the Service Provider, or for which the Service Provider is otherwise responsible, in accordance with the initial transition plan attached to this Agreement as **Schedule 2** *(Transition Plan)*, as such transition plan may be amended, modified and supplemented in accordance with the provisions of Section 3.4 (*Modifications to Transition Plan*) (collectively, the "**Transition Plan**"); and

(c) the Service Provider will be responsible for the overall management and implementation of the Transition, including coordinating, planning and implementing the Transition in accordance with the Transition Plan and this Agreement.

3.4 Modifications to Transition Plan.

Notwithstanding the level of detail contained in the initial Transition Plan, the Parties acknowledge that the initial Transition Plan may require modifications after the execution of this Agreement. Such modifications will be agreed to by the Parties in accordance with the Transition Governance Process, and once agreed to through the Transition Governance Process, such modifications will be incorporated into the Transition Plan, and the Transition Plan will be deemed to be amended accordingly (including amending **Schedule 2** *(Transition Plan)*). For greater clarification, the Parties confirm that any changes to the following in respect of the Transition Plan will require the joint Approval of the Parties through **[insert appropriate level of approval for significant changes, e.g., the AMO, the Joint Executive Committee, etc.]**:

(a) the Hand-Over Date; and

(b) the scope of the Services to be provided by the Service Provider as of the Hand-Over Date.

3.5 Transition Management.

During the Transition Period and for one month after the Hand-Over Date, each Party will assign a transition management team (each a "**Transition Management Team**"), comprised of the members as set forth in **Schedule 3** *(Transition Management and Governance)*, who will be primarily dedicated to the implementation of the Transition. The guiding principles, responsibilities and meeting process for meetings between members of each Transition Management Team will be as set forth in **Schedule 3** *(Transition Management and Governance)*. For greater clarification, **Schedule 3** *(Transition Management and Governance)* includes a governance process to monitor progress and identify any issues or circumstances that may impact the schedule set forth in the Transition Plan (the "**Transition**

Governance Process"). Any potential delays or circumstances that may adversely affect the Transition will be escalated in accordance with the Transition Governance Process in lieu of the Change Order Process.

3.6 Completion of Transition Plan.

Subject to Sections 3.9 (*Failure to Complete Transition Plan*) and 3.12 *(Effect of Termination Prior to Hand-Over Date*), the transfer of the provision and performance of the Services to the Service Provider will be subject to the completion of the requirements of the Transition Plan before the Hand-Over Date. Such requirements of the Transition Plan will be completed at such time as:

(a) all components of the Transition Plan that are required under the terms of the Transition Plan to be completed prior to the Hand-Over Date have been completed; or

(b) the Service Provider and the Province, through the Transition Governance Process, have jointly waived the requirement to complete any such component of the Transition Plan that has not been completed prior to the Hand-Over Date, or have transferred the obligation of the Service Provider (or other applicable Person) to complete the same after the Hand-Over Date.

The Service Provider will complete all components of the Transition Plan (if any) that are required under the terms of the Transition Plan to be completed after the Hand-Over Date, within the times indicated in the Transition Plan.

3.7 Transition Costs.

Other than the payment of the applicable Fees expressly set forth in Article 15 (*Fees and Payment Terms*) which are the responsibility of the Province, the Service Provider is responsible for all of the costs incurred by the Service Provider (or its Subcontractors) for completing the Transition Plan, including all direct and indirect costs incurred by the Service Provider (or its Subcontractors) in connection with the implementation of the Transition Plan, and the overall management of the Transition Plan, but excluding therefrom:

(a) those costs, if any, identified in the Master Transfer Agreement as being the responsibility of the Province; and

(b) those costs incurred by the Province in connection with the Transition Plan.

3.8 Work-in-Progress Projects.

The Parties acknowledge that there are certain Work-in-Progress Projects existing as of the date of this Agreement in respect of which there may be work that will not be completed by the Hand-Over Date, and that will constitute work-in-progress as of such date, as more particularly described in **Schedule 4** *(Work-in-Progress Projects)*. The Parties will handle the Work-in-Progress Projects in accordance with the following principles:

(a) the Province will have financial and operational responsibility for the Work-in-Progress Projects prior to the Hand-Over Date; and

(b) from and after the Hand-Over Date, the Service Provider will assume operational responsibility for the Work-in-Progress Projects that have not been completed by the

Hand-Over Date, which will be paid for in accordance with the provisions of **Schedule 23** *(Fees)*.

3.9 Failure to Complete Transition Plan.

If the Transition Plan is not completed, as applicable, by the Hand-Over Date (which completion will be determined in the manner specified in Section 3.6 *(Completion of Transition Plan)*), then the provisions set forth in Sections 3.10 *(Delays Caused by Province)*, 3.10 *(Delays Caused by Service Provider)*, and 3.12 *(Effect of Termination Prior to Hand-Over Date)* will apply, as applicable under the circumstances; provided that if the Parties are unable to agree upon which Party caused the delay, then the matter of fault for purposes of determining whether the delay was caused by one Party or the other, will be deemed to be a Dispute and will be determined in accordance with the Dispute Resolution Process under Article 27 *(Dispute Resolution)*. For greater clarification, no Party will be deemed to have failed to perform its obligations under the Transition Plan where such performance is dependent upon the performance by the other Party of that other Party's obligations under the Transition Plan, in circumstances where that other Party has failed to so perform.

3.10 Delays Caused by Province.

If the failure to complete the Transition by the Hand-Over Date is due to the fault or delay of the Province (in circumstances where the Parties have not jointly waived the requirement to complete the incomplete components of the Transition Plan pursuant to the provisions of Section 3.6 *(Completion of Transition Plan)*), then the provisions of **[insert applicable section from the schedule] Schedule 5** *(Special Terms)* will apply.

3.11 Delays Caused by Service Provider.

If the failure to complete the Transition by the Hand-Over Date is for any reason other than the fault or delay of the Province (in circumstances where the Parties have not jointly waived the requirement to complete the incomplete components of the Transition Plan pursuant to the provisions of Section 3.6 *(Completion of Transition Plan)*), then the Province may, in its sole and absolute discretion, do one or more of the following:

(a) *Postponement* – postpone the Hand-Over Date to such later date as the Province may select by giving to the Service Provider as much prior written notice of such postponed Hand-Over Date as may be possible under the circumstances, which postponed Hand-Over Date may be further extended by the written agreement of the Parties, but in any event will be no later than **[insert drop dead date]** (the "**Final Hand-Over Date**"), in which event:

(i) the Service Provider will complete the Transition in accordance with the terms of the Transition Plan, applied *mutatis mutandis*, and to the satisfaction of the Province on, or before such postponed Hand-Over Date,

(ii) the provisions of **[insert section from the schedule containing any applicable remedies available to the Province as a result of the delay] Schedule 5** *(Special Terms)* will apply, and

(iii) if the Transition is not completed by such postponed Hand-Over Date (as may be extended in accordance with paragraph (a) above up to and no later than the Final Hand-Over Date), then the Province may give written notice of termination of

this Agreement to the Service Provider, in which event the provisions of Section 3.12 (*Effect of Termination Prior to Hand-Over Date*) will apply; or

(b) *Partial Commencement* – if the Transition is substantially complete and it is reasonably practicable to do so, give written notice to the Service Provider to commence all available Services on the Hand-Over Date (the "**Partial Commencement**"), in which case:

(i) the provisions of **[insert section from the schedule containing any applicable remedies available to the Province as a result of the delay] Schedule 5** (*Special Terms*) will apply, and

(ii) the Service Provider will complete the outstanding obligations under the Transition Plan in accordance with its terms, applied *mutatis mutandis*, within 30 days of the Partial Commencement of the Services on the Hand-Over Date (unless otherwise agreed to by the Parties in writing), provided that there will be no Partial Commencement unless the Parties first agree upon the Fees to be paid by the Province to the Service Provider with respect to such Partial Commencement.

3.12 Effect of Termination Prior to Hand-Over Date.

If this Agreement is terminated prior to the Hand-Over Date, then the following provisions will apply:

(a) the obligations of the Parties to continue to pursue the transactions and the contractual relationship contemplated in this Agreement and in the other Transaction Documents will immediately terminate and cease to be of any further force or effect;

(b) this Agreement will terminate and cease to be of further force or effect subject to survival of those provisions specified in Section 33.11 (*Survival*) of this Agreement;

(c) each of the other Transaction Documents, if executed and delivered, will terminate and cease to be of any further force or effect subject to survival of any provisions contemplated therein or herein to survive termination of the applicable Transaction Documents, and any assets transferred in respect of such Transaction Documents prior to such date will be transferred back to the original Party on the same terms as initially transferred;

(d) the Service Provider will, forthwith after the Termination Date, return to the Province (or at the direction of the Province destroy) all of the Province Confidential Information and Province Records provided to the Service Provider prior to the Termination Date (including prior to the execution of this Agreement pursuant to the JSDA), and will not retain and will destroy all copies thereof which the Service Provider (or any Subcontractor, agent, consultant or Person working for or hired by or on behalf of the Service Provider in connection with this Agreement, the Transaction Documents and the transactions contemplated herein and therein) may have made or caused to be made;

(e) where this Agreement is terminated as a result of a failure to complete the Transition by the Hand-Over Date for any reason other than the fault or delay of the Province, then the Service Provider will not be entitled to receive any payment or compensation from the Province; and

(f) where this Agreement is terminated by the Province as a result of a failure to complete the Transition by the Hand-Over Date due solely to the fault or delay of the Province, then the Service Provider will not be entitled to receive any payments or other compensation from the Province except as expressly provided for in **Schedule 38** *(Termination Fees)* in respect of a Termination effected pursuant to this Section 3.12 (*Effect of Termination Prior to Hand-Over Date*).

ARTICLE 4 – SERVICES

4.1 Overview of Services.

Subject to a Partial Commencement of the Services pursuant to Article 3 (*Initial Transition*), as may otherwise be agreed to by the Parties in accordance with the Change Order Process, and as may be transformed and otherwise changed in accordance with the provisions of this Agreement during the Term, the Service Provider will provide to the Province, and the Province will obtain from the Service Provider, the following services from and after the Hand-Over Date (or from and after such other date as indicated below), upon the terms and conditions set forth in this Agreement (collectively, the "**Services**"):

(a) the Transition Services, as more particularly described in Article 3 (*Initial Transition*), from and after the Effective Date;

(b) the basic services described as such in **Schedule 6** *(Basic Services)* (which includes the inherent services described in Section 4.2 (*Included or Inherent Services*), as such Schedule may be amended and supplemented by the Parties from time to time in accordance with this Agreement (collectively, the "**Basic Services**");

(c) the transformed services in accordance with Article 6 (*Transformation*), being the Basic Services as described in **Schedule 6** *(Basic Services)* as transformed pursuant to the Transformation Plan (collectively, the "**Transformed Services**");

(d) the Termination Services, as more particularly described, and within the times indicated, in Article 29 (*Termination Services*);

(e) such other services or additional services as may be agreed to by the Parties pursuant to the Change Order Process; and

(f) all such other or additional services as set forth or otherwise described in this Agreement.

4.2 Included or Inherent Services.

The Parties acknowledge that there are functions or tasks not specifically listed or described in this Agreement that are customarily required for the proper performance and provision of the Services (as the same may be improved, changed or transformed as contemplated under this Agreement), or as may otherwise be required to perform the Services in a manner consistent with the performance thereof prior to the Hand-Over Date. Without limiting the foregoing and subject to the provisions of this Section, such functions or tasks will be deemed to be implied or included in the scope of the Services to the same extent and in the same manner as if those functions or tasks had been specifically described in this Agreement. Notwithstanding the foregoing, this Section is not intended to expand the scope of the Services beyond the Services described in this Agreement, or to require a higher standard of Service delivery than that which is otherwise described in this Agreement.

4.3 Language of Services.

The Service Provider will provide all of the Services in English, and in such other languages and with such other special arrangements to accommodate customers with visual, hearing and other similar forms of special needs, as set forth in **Schedule 7** *(Language of Services)*.

4.4 Standard of Care.

Unless specifically provided otherwise in this Agreement (or in any schedules attached to this Agreement), the Service Provider will provide the Services under this Agreement using the standard of care of a reasonable service provider performing similar services in comparable circumstances.

4.5 Services and Program Changes.

All changes, modifications, amendments or supplements to the Services provided by the Service Provider to the Province under this Agreement will be undertaken in accordance with the Change Order Process and any other express provisions of this Agreement that contemplate changes to the Services.

4.6 Service Recommendations.

As part of the Services, the Service Provider will, from time to time as it may deem appropriate, but not less frequently than annually, make recommendations to the Province for improvements to the Services based on changes and trends in the **[insert industry in which the Services are being provided]** field and available new technologies, and implement any of such recommendations Approved by the Province in accordance with the Change Order Process.

4.7 Quality Management.

In providing the Services to the Province during the Term, the Service Provider will:

(a) be responsible for implementing and carrying out continuous improvement and quality management for all of the Services;

(b) establish quality assurance programs that encompass continuous improvement of the Services in addition to an ongoing quality assessment of the Services;

(c) maintain an ongoing focus on the satisfaction of the Province and the Stakeholders, as well as other users of the Services, by monitoring and evaluating trends that develop in the performance of the Services (as indicated through complaint processes or otherwise), and by making recommendations to the Province in respect thereof; and

(d) such activities will be performed entirely by the Service Provider at its own expense and will not require the resources of the Province or the payment of any additional Fees without the Approval of the Province.

4.8 Documentation.

The Service Provider will deliver to the Province a detailed and comprehensive operational procedures manual in respect of the Services (the **"Manual"**), in a form and substance that is subject to the Province's prior consultation, and containing the matters referred to in Section 4.9 *(Manual Requirements)*, by the end of the Transition Period ***[- or- "within • days of the Hand-Over Date"]***. The Service Provider will periodically, but not less than **[insert time period e.g., quarterly, every six**

months, etc.] unless otherwise agreed by the Province, update the Manual to reflect changes in the operations or procedures described in the Manual. The Service Provider will provide the Province with the updates of the Manual on a timely basis, and within the period required for such updates to be made, for consultation with the Province. For greater clarification, the Parties acknowledge that the Manual is intended to describe to the Province how the Services will be performed, and will in no event be interpreted so as to relieve the Service Provider of any of its performance obligations under this Agreement. The consultation with the Province under this Section 4.8 (*Documentation*) is not intended to, and will not be deemed to, shift the risk and responsibility for the business operations in performing the Services from the Service Provider to the Province, and the Parties acknowledge and agree that the responsibility and risk thereof will remain at all time with the Service Provider.

4.9 Manual Requirements.

The Manual will describe or include the following:

(a) the procedures associated with the business processes and technology support services that the Service Provider will undertake in order to provide the Services;

(b) the methods of operation and procedures the Service Provider will use to perform the Services, such as network topologies, security administration, system configurations, call centre processes, human resource functions, business processes and associated documentation that provides further details of such activities, as applicable (including, for example, user support manuals, job scheduling procedures, specifications and updates of such materials); and

(c) current documentation with respect to the Systems, business processes, and processes in support of the operations and procedures used to deliver the Services (which documentation will be sufficient to enable the Province, or another service provider that is reasonably skilled in the provision of services similar to the Services, to fully assume the provision of the Services), and the Manual will detail how such documentation will be maintained.

4.10 Knowledge Transfer.

The Service Provider acknowledges that the Province needs to retain an appropriate level of understanding regarding the manner in which the Services are delivered throughout the Term. As part of the Basic Services, the Service Provider will provide the Province with ongoing knowledge transfer with respect to the Services in the manner Approved through the Governance Process or as otherwise requested by the Province from time to time. The Service Provider will provide such knowledge transfer to the Province at the level of information and detail as may be required by the Province to ensure that the Province is a well informed customer regarding the manner in which the Services are delivered. At the request of the Province, the Service Provider will provide any new Province staff (who have duties related to the Services or the Service Provider) with an orientation and training regarding the manner in which the Services (or such portion of the Services as may be applicable under the circumstances) are delivered by the Service Provider, and at such mutually scheduled times as may be reasonably agreed to by the Parties through the Governance Process. The Service Provider will also provide the Province and its staff with information and general training sessions regarding any significant process or Systems changes that may occur in respect of the Services throughout the Term.

4.11 Province Retained Responsibilities.

During the Term (and without limiting any other provisions of this Agreement regarding the responsibilities of the Province), the Province will remain responsible for and will retain control of the following:

(a) setting all Province Policies and guidelines including, without limitation, those relating to the Services, records management, and privacy and security;

(b) all media relations, including the Approval of the Service Provider media communications and Stakeholder communications in accordance with Article 10 (*Branding and Communications*);

(c) the exercise of powers for and on behalf of Her Majesty the Queen in Right of the Province of British Columbia, as represented by the Minister of Labour and Citizens' Services;

(d) **[insert other as applicable to the transaction]**; and

(e) such other direct responsibilities as may be expressly contemplated in this Agreement.

The Parties acknowledge that these responsibilities are vested solely in the Province. The Service Provider has no right or obligation to exercise any responsibilities of the Province set forth in this Section and is not accountable for actions taken by the Province in respect of the same. For greater clarification, where the Province exercises its responsibilities under this Section 4.11 (*Province Retained Responsibilities*) and such exercise affects the Service Provider in the manner contemplated in the Change Order Process, then the provisions of Article 7 (*Change Order Process*) will apply, as applicable.

4.12 Failure of Province to Perform Retained Responsibilities.

In the event of (i) a failure by the Province to perform its obligations under this Agreement (other than a failure to make payments in accordance with Section 28.3 (*Material Breach by Province*), (ii) a failure by the Province to provide services to the Service Provider as specifically provided in this Agreement, if any, to the extent that the Services are contingent upon the performance by the Province thereof, or (iii) the Province Intellectual Property utilized or otherwise accessed by the Service Provider under license or access rights pursuant to Section 19.5 (*Use of Province Software for the Services*) infringing the Intellectual Property rights of a third party, such that the Service Provider is unable to utilize such Province Intellectual Property, then the following provisions will apply:

(a) the Service Provider will notify **[insert title of Province representative for this particular notice requirement]** as soon as possible, and in any event within five (5) Business Days from the date the Service Provider discovers that such failure or infringement has occurred, providing details with respect to such failure or infringement (such as the specific obligation or co-operation sought, the individuals from whom it was sought, and the date such request was made);

(b) the Service Provider and the Province, through the Governance Process, will promptly meet in order to discuss and resolve, if possible, the failure or the infringement;

(c) unless the Province contests the Service Provider's assertion that such failure or infringement has occurred, the Province will address such failure, make reasonable efforts to either negotiate a license or access rights in respect of the Province Intellectual

Property in question, provide a "workaround" to address the failure or infringement, or provide alternative Intellectual Property as a replacement for the infringing Province Intellectual Property, all as applicable under the circumstances;

(d) if such failure of the Province or infringement has a material impact on the delivery and performance of the Services or on the cost of providing the Services, then effective as of the date that the notice of the failure or infringement is delivered to the Province in accordance with paragraph (a) above, the Service Provider and the Province will adjust the Fees, time frames for performance, Service Levels or Services, as applicable and to the extent affected, either on a temporary basis or a long term basis, in accordance with the Change Order Process;

(e) if the Service Provider does not so notify the Province of the failure or infringement as set forth in this Section, then no such Mandatory Change will be deemed to have occurred, and such failure or infringement on the part of the Province will not constitute an excuse or defence for the Service Provider's failure to perform its obligations under this Agreement;

(f) for greater clarification, the Parties acknowledge that the Service Provider has the right to elect not to immediately deliver notice to the Province under paragraph (a) above for minor failures, with such election in no way restricting the Service Provider from subsequently delivering a notice under paragraph (a) above that is in respect of all such minor failures (to the extent that they continue to impact delivery of the Services), all of such failures thereafter being deemed, for the purposes of this Section, to be a single failure by the Province to perform in accordance with its obligations under this Agreement;

(g) any failure of the Province Shared Infrastructure will not be governed by this Section but will instead be governed by the provisions set forth in Article 20 (*Province Shared Infrastructure*); and

(h) except as specifically provided otherwise in this Agreement, the application of the foregoing provisions will constitute the sole remedy of the Service Provider in respect of such failure or infringement by the Province.

4.13 Restrictions on Shared Environment.

Unless expressly provided elsewhere in this Agreement or upon the Approval of the Province, the Service Provider will ensure that all Systems and premises that are used to provide the Services are not in any manner shared or otherwise utilized to provide services to any other Person unless expressly Approved by the Province. With respect to any shared Systems or premises that are Approved by the Province, the Service Provider will ensure that all such Systems and premises are segregated and not accessible at any time by any Persons other than those expressly authorized by or in accordance with this Agreement, and that such Systems and premises are not used for any purposes except for those expressly Approved by the Province. Without limiting the generality of the foregoing, the Service Provider will at all times comply with the privacy, confidentiality and security obligations as set forth in **Schedule 24** *(Privacy Obligations)* and as otherwise set forth in this Agreement. At no time and under no circumstances will any Personal Information or Province Confidential Information be shared or otherwise accessible by any shared System other than the Province Shared Infrastructure (to the extent applicable).

ARTICLE 5 – SERVICE AND DATA LOCATIONS

5.1 Overview of Service Locations.

No Services will be provided or performed by the Service Provider at any location outside of British Columbia (or elsewhere in Canada as may be permitted under or pursuant to this Agreement) and no Personal Information will be accessed, used, stored, transmitted or otherwise made available in any manner outside of Canada, and no Person outside of Canada will have access in any manner to the Personal Information, except as may be specifically permitted under the *Freedom of Information and Protection of Privacy Act* (British Columbia) and Approved in writing by the Province from time to time.

5.2 Service Locations.

The addresses at which any Personal Information will be accessed, used, stored, transmitted or otherwise made available by the Service Provider or its Subcontractors, or from where any Services will be performed (collectively, the "**Service Locations**"), are set forth in the attached **Schedule 8** *(Service Locations)*. The Service Provider will not store any Personal Information databases except in those locations set forth in **Schedule 8** *(Service Locations)* without the Province's Approval, and the Service provider will ensure that its Subcontractors do not access, use, store, transmit or otherwise make available any Personal Information at any other locations unless the Service Provider provides the Province with prior written notice thereof, and provided that such locations are within British Columbia (or elsewhere in Canada as may be permitted under or pursuant to this Agreement). For greater clarification, nothing contained in this Section will permit or otherwise enable the Service Provider (or any of its Subcontractors) to perform the Services from a location outside of British Columbia unless permitted under or pursuant to this Agreement or otherwise Approved by the Province.

5.3 Relocation of the Service Provider Service Locations.

The Service Provider may relocate all or a part of the Service Centre or the Services at any time upon prior written notice thereof to the Province, provided that:

(a) the Service Provider will not permit its Personnel or any External Personnel to work from home or engage in other similar remote telecommunicating activities, where the same involve the use of Personal Information, without the prior Approval of the Province through the Change Order Process; and

(b) the relocation of all or any portions of the Services or the Service Centre will be subject to the Approval of the Province, which will not be unreasonably withheld (acknowledging that the Province will grant or withhold such Approval having regard to the interests of the Province and the Stakeholders).

5.4 Service Location Policies.

To the extent applicable, at all times while accessing any premises of the other Party (including the premises of any applicable subcontractors of that other Party) in connection with the Services being performed under this Agreement, or as may otherwise be contemplated under this Agreement, each Party will, and will cause their respective personnel, external personnel, subcontractors, representatives or other parties for whom they are responsible at law or under the terms of this Agreement to, comply with any standard workplace security, safety, operational and other similar policies and procedures applicable to visitors for such Party, as may be notified by each Party to the other from time to time. The foregoing will not in any way limit or otherwise prohibit the Province from exercising its rights under Article 22 (*Audit Rights*).

ARTICLE 6 – TRANSFORMATION

6.1 Transformation Obligations.

The Service Provider will complete the Transformed Services without any material disruptions to the other Services (except to the extent that such other Services are intended to be superseded, replaced or transformed by the Transformed Services). The Service Provider will be responsible for all costs incurred by the Service Provider in connection with the performance of the Transformed Services, including license fees for Software licensed by the Service Provider, unless expressly agreed otherwise by the Province in accordance with the Change Order Process or the terms of this Agreement.

6.2 Transformation Plan.

The Transformation will be conducted in accordance with the transformation plan prepared by the Service Provider, including the completion dates set forth in the transformation plan, an initial copy of which is attached as **Schedule 10** *(Transformation Plan)*, and as such initial transformation plan may be amended, modified and supplemented as contemplated in Section 6.3 *(Modifications to Transformation Plan)* (collectively, the "**Transformation Plan**"). Any such modifications to the Transformation Plan, once agreed to by the Parties in accordance with Section 6.3 *(Modifications to Transformation Plan)*, will be incorporated into the Transformation Plan, and the Transformation Plan will be deemed to be amended accordingly (including amending **Schedule 10** *(Transformation Plan)*).

6.3 Modifications to Transformation Plan.

Notwithstanding the level of detail contained in the initial Transformation Plan attached as **Schedule 10** *(Transformation Plan)*, the Parties acknowledge that the initial Transformation Plan may require modifications after the execution of this Agreement. Such modifications will be agreed to by the Parties in accordance with the Change Order Process, and once agreed to through the Change Order Process, any such modifications will be incorporated into the Transformation Plan, and the Transformation Plan will be deemed to be amended accordingly. In connection with any such modifications to the Transformation Plan, the Service Provider will ensure that the Transformation Plan, as so modified, adequately addresses the following (collectively, the "**Critical Issues**") to the satisfaction of the Province:

(a) policy compliance and operational impact;

(b) impact on and interface with customers of the Services and Stakeholders;

(c) standards adherence and privacy and security;

(d) a detailed description of each Stage and applicable completion dates for each Stage;

(e) a detailed description of the Transformed Services; and

(f) **[list other critical issues relevant to the project]**.

6.4 Disputes Regarding the Transformation Plan.

If modifications are required to be made to the Transformation Plan as contemplated under Section 6.3 (*Modification to Transformation Plan*), and the Parties are unable to agree upon all or any matter relating to such modifications to the Transformation Plan in accordance with the Change Order Process, then the matter will be deemed to be a Dispute and will be settled between the Parties in accordance with the process described in Section 27.3 (*Special Arbitration*).

6.5 Transformed Services.

The Service Provider will be responsible for overall management and implementation of the Transformation, including coordinating, planning and implementing the Transformation in accordance with the Transformation Plan and this Agreement. The Service Provider will minimize any disruption to the Services and the business operations of the Province and the Stakeholders in connection with such Transformation.

6.6 Acceptance Testing.

The Acceptance Test procedures in this Section and in the Transformation Plan apply to each Stage of the Transformation, as the same are completed from time to time, as follows:

(a) subject to specific timelines otherwise set forth in the Transformation Plan, or as otherwise agreed by the Parties, the Province will have no less than **[insert number]** Business Days from the date that the deliverables are made available to the Province for each Stage of the Transformation to perform (or cause the Service Provider to perform, to the satisfaction of the Province) the Acceptance Tests to verify that, in all material respects, the deliverables conform with the Transformation Plan, all requirements of this Agreement and all related requirements (including Province Policy compliance), and that the Critical Issues are adequately addressed, and the Service Provider will cooperate fully with the Province and take all necessary steps and do such things as may be necessary to facilitate, assist or complete (as applicable) the Acceptance Test at the Province's request and without the payment of any additional Fees in respect thereof;

(b) subject to specific timelines otherwise set forth in the Transformation Plan, or as otherwise agreed by the Parties, the Province will have no less than **[insert number]** Business Days from the date that all deliverables for the entire Transformation have been delivered to the Province to perform (or cause the Service Provider to perform, to the satisfaction of the Province) the Acceptance Tests to verify that in all material respects, the deliverables as a whole conform with the Transformation Plan and that the Critical Issues are adequately addressed, and the Service Provider will cooperate fully with the Province and take all necessary steps and do such things as may be necessary to facilitate, assist or complete (as applicable) the Acceptance Test at the Province's request and without the payment of any additional Fees in respect thereof;

(c) promptly upon becoming aware of any Non-Compliance in connection with the Transformation, the Province will notify the Service Provider of the Non-Compliance and will provide the Service Provider with all information reasonably available to the Province with respect to the Non-Compliance;

(d) the Service Provider will use its best efforts to correct all Non-Compliance issues and to deliver the corrected deliverables to the Province within **[insert number]** Business Days after the conclusion of the relevant Acceptance Test (or such other period of time as may be specified in the Transformation Plan or otherwise agreed by the Parties, acting reasonably under the circumstances). Where such efforts cannot correct all Non-Compliance issues within such **[insert number]** Business Day period, then within such period the Service Provider will deliver to the Province a written plan describing how and within what time periods it will remedy such Non-Compliance, with the Service Provider continuing to be bound to use its best efforts to correct the balance of such Non-Compliance as expeditiously as possible. The Province will have a further **[insert number]** Business Days from the date on which the corrected deliverables are delivered

(or such other period of time as may be specified in the Transformation Plan or otherwise agreed by the Parties) in which to conduct or cause the Service Provider to conduct (in accordance with paragraphs (a) and (b) above, as applicable) additional Acceptance Tests to determine whether the Non-Compliance is corrected. The reporting, correction and re-testing process will, subject to Section 6.7 (*Delay in Completion of Transformation*), be repeated until all Non-Compliance is corrected;

(e) subject to this Section and to Section 6.7 (*Delay in Completion of Transformation*), the deliverables for a given Stage will be accepted by written notice from the Province to the Service Provider, and the Province agrees to promptly give such notice when the deliverables conform to the Transformation Plan and address all Critical Issues and remedy all Non-Compliance to the satisfaction of the Province (the date of delivery of written notice from the Province to the Service Provider is referred to as the "**Acceptance Date**"); and

(f) the Province will promptly provide written notice to the Service Provider when the deliverables for the entire Transformation have been made available to the Province, the Province has completed (or caused the Service Provider to complete) the Acceptance Tests, the deliverables conform with the Transformation Plan, and all Non-Compliance reported during the Acceptance Tests is corrected to the satisfaction of the Province. Such notice of acceptance will constitute final acceptance of the deliverables.

6.7 Delay in Completion of Transformation.

Each Stage of the Transformation will have a completion date for the particular Stage as set forth in the Transformation Plan. Where the Acceptance Date for any Stage is past the applicable completion date for the Stage, then credits will be granted by the Service Provider to the Province (the "**Transformation Credits**") in accordance with the provisions set forth in **Schedule 10** *(Transformation Plan)*. The Province may deduct or off-set the Transformation Credits against the Fees payable by the Province to the Service Provider under this Agreement.

ARTICLE 7 – CHANGE ORDER PROCESS

7.1 Ordinary Course Changes.

The Parties acknowledge and agree that the **[insert industry sector, as applicable to the outsourcing]** industry operations and activities of the Province that are the subject of the delivery of Services pursuant to this Agreement are subject to constant changes in the ordinary course of such operations and activities, which changes do not have a material impact on the following (collectively, the "**Ordinary Course Changes**"):

(a) the delivery and performance of the Services; or

(b) the cost of providing the Services .

The Ordinary Course Changes are within the scope of the Services contemplated under this Agreement and will not result in additional Fees being payable by the Province to the Service Provider. The Ordinary Course Changes may be implemented without the need for a formal Change Order. Notwithstanding the foregoing, the Service Provider will maintain a record of each Ordinary Course Change that occurs in the Services, and will provide the Province, through the Governance Process, with **[insert time period e.g., monthly, quarterly]** reports detailing the same.

7.2 Province Initiated Ordinary Course Changes.

The Province may require the Service Provider to implement any Ordinary Course Change by written notice to the Service Provider of such change, in which event the following provisions will apply:

(a) no formal documentation requesting the Ordinary Course Change is required and the Province may request the Ordinary Course Change by any form of written notice (including electronic forms of notice) to the Service Provider;

(b) the Approval or agreement of the Service Provider to an Ordinary Course Change requested by the Province is not required, and the Service Provider will implement the Ordinary Course Change as soon as reasonably practicable following receipt by the Service Provider of a written notice from the Province requesting it to do so; and

(c) the Parties will cause a record of each Ordinary Course Change to be maintained as contemplated in Section 7.1 (*Ordinary Course Changes*).

7.3 Other Changes.

In addition to the Ordinary Course Changes, the Parties acknowledge that certain changes may be required or desirable which exceed or are otherwise outside of the definition of Ordinary Course Changes. Such changes may include, without limitation, the following:

(a) the addition or removal of Material Services ;

(b) changes to a Service Level (including the addition or removal of Services Levels);

(c) a material change to the technology or Systems used in the performance of the Services;

(d) a permanent change that has a material impact on the delivery or cost of the Services;

(e) a change that has an material impact on the Privacy Obligations;

(f) a change in the locations from where the Services are primarily performed; and

(g) any other matter that the Parties may agree as properly being the subject of the Change Order Process.

7.4 Change Request.

Either Party may initiate the change process described in Sections 7.4 (*Change Request*) to 7.12 (*Record of Changes*) (collectively, the "**Change Order Process**") in connection with a change described in Section 7.3 (*Other Changes*) by submitting to the other Party, through the Governance Process, **[NOTE – Governance Process to specifically state, for each party, who has authority to issue Change Requests, and to whom they must be sent]** a written notice signed by the initiating Party, which notice will include all relevant information reasonably required for the proper consideration of such change or for the commencement of the Change Order Process in respect thereof (each, a "**Change Request**").

7.5 Change Request Process.

Following the delivery of a Change Request by one Party to the other, the following will apply:

(a) the Parties will meet together through the Governance Process to clarify the Change Request and confirm the requirements of the Change Request including, without limitation, details regarding the time requirements to consider the Change Request (it being acknowledged by the Parties that the time required may vary depending upon the nature and complexity of the proposed change);

(b) upon receipt of a Change Request from the Province, the Service Provider will prepare a proposal (the "**Proposal**") within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process, acting reasonably and having regard to the nature and complexity of the Change Request in question), which Proposal will include a privacy assessment of the collection, use, disclosure and retention of Personal Information and a threat and risk assessment (in such form as may be required by the Province), as well as a description of the impact of the proposed change on the following (to the extent applicable having regard to the nature of the proposed change):

(i) the costs of implementation,

(ii) the rights and obligations of the Parties under this Agreement with respect to, or as a result of, the proposed change,

(iii) the Services,

(iv) the Service Levels,

(v) any technology, Systems or operations of the Service Provider used in the Services, the Province, the Stakeholders or any customers of the Services,

(vi) an increase or decrease to the Fees payable under this Agreement,

(vii) the Privacy Obligations, and

(viii) any other relevant matter related to this Agreement that will be materially impacted (both positively and negatively);

(c) if the Service Provider initiates the Change Request, then the Service Provider will prepare and deliver a Proposal to the Province within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process, acting reasonably and having regard to the nature and complexity of the Change Request in question) following the meeting of the Parties to clarify the Change Request, as contemplated in paragraph (a) above;

(d) the Province will provide the Service Provider with a written response to the Proposal within ten (10) Business Days (or such longer or shorter period of time as agreed to by the Parties through the Governance Process) of receipt of the Proposal from the Service Provider, indicating the Province's Approval of the Proposal, its rejection of the Proposal (indicating the reasons therefor), or the terms of a counter proposal acceptable to the Province;

(e) any Proposal Approved by the Province will constitute a Change Order, and will be implemented by the Service Provider in accordance with the particulars of the Change Order;

(f) the Service Provider will be required to respond to all Change Requests received from the Province and to prepare a Proposal in respect thereof;

(g) the Service Provider will not reject a Change Request initiated by the Province unless the Service Provider is unable to make the changes contemplated in the Change Request as a result of technical impediments that are commercially unreasonable to overcome, or the Change Request will result in a material adverse effect on the Service Provider's ability to meet Service Levels, comply with the Privacy Obligations or comply with other material terms or conditions of this Agreement (each an "**Adverse Impact**"). The Service Provider will provide the Province with a written explanation of any Adverse Impact stating in detail the particulars of the Adverse Impact and suggesting reasonable alternatives or workarounds (to the extent possible) for consideration by the Province in respect thereof; and

(h) if the Province requires that the Change Request be implemented as requested, notwithstanding the Adverse Impact to the Service Provider, then the impact of the Change Request on the Fees, the Service Levels, the Privacy Obligations or other material terms and conditions of this Agreement will be addressed through the Governance Process. If a mutually acceptable resolution is not reached in respect of the proposed Change Request, then the matter will be treated as a Dispute to be resolved pursuant to the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*).

7.6 Change Request Impact on Fees.

If a Change Request has an impact on the Fees that may result in either an increase or decrease to the Fees, then the Parties will determine any increase or decrease to be made to the Fees as a result of such impact in a manner that is consistent with the determination of the amounts as set forth in the Economic Model.

7.7 Mandatory Changes.

The Province may require the Service Provider to implement a Change Request before it has become a Change Order (each a "**Mandatory Change**") in situations where:

(a) the Parties are unable to agree upon the Change Request and associated Proposal for any reason;

(b) due to time constraints, the Parties are unable to use, fully complete or otherwise commence the processes set forth in Sections 7.4 (*Change Request*) to Section 7.6 (*Change Request Impact on Fees*); or

(c) due to the urgency of the circumstances surrounding the need for the Mandatory Change, the Province requires that the Service Provider implement the changes forthwith.

The Mandatory Changes will be implemented by the Parties in accordance with the provisions of Section 7.8 *(Implementation of Mandatory Changes).*

7.8 Implementation of Mandatory Changes.

The Province may require the Service Provider to implement a Mandatory Change by the delivery of a written request (each, a "**Mandatory Change Request**") to the Service Provider, in which case the following provisions will apply:

(a) the Mandatory Change Request will comply with the requirements of Section 7.4 *(Change Request)*;

(b) the Approval or agreement of the Service Provider to the Mandatory Change Request is not required;

(c) the Mandatory Change Request will immediately become a Change Order for the purposes of Section 7.9 *(Change Orders)* upon the issuance by the Province, and the Service Provider will implement the Mandatory Change following receipt of the Mandatory Change Request from the Province, as soon as reasonably practicable to do so;

(d) if, as a result of the Mandatory Change, the Fees are to be increased, decreased or otherwise changed, or any Service Levels, time frames, Privacy Obligations or Services will be impacted, and a determination must be made regarding the particulars of such increase, decrease, change or impact, then the following procedures will apply:

(i) forthwith after receipt from the Province of a Mandatory Change Request in respect of a Mandatory Change, the Service Provider will provide the Province with its proposed adjustment to the Fees and any impact on Service Levels, time frames, Privacy Obligations and Services, in all cases with supporting documentation including, without limitation, detailed information, analysis and back-up support regarding any increase or decrease to the Fees (the "**Impact Assessment**"),

(ii) after the Province has received and reviewed the Impact Assessment from the Service Provider, the Province will, acting reasonably, and after due consideration of the proposed Impact Assessment, and by separate written notice to the Service Provider, set the adjustment to the Fee or such other adjustment or change to the Service Levels, time frames, Privacy Obligations and Services, which adjustment or change will take effect immediately with retroactive effect to the date of the implementation of the Mandatory Change, to the extent applicable under the circumstances,

(iii) if the Service Provider has a Dispute with respect to such adjustment or change, then the Dispute will be settled pursuant to the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution),* and

(iv) the adjustment or change determined by the Province will apply until any Dispute in respect thereof has been resolved between the Parties, whereupon the Parties will make such adjustments as between themselves as may be necessary to give effect to the resolution of the Dispute, retroactive (to the extent possible) to the date of the implementation of the Mandatory Change giving rise to such Dispute;

(e) the costs of implementing a Mandatory Change will be borne by the Service Provider, unless otherwise determined by the Province, acting reasonably, as indicated in its Mandatory Change Request issued with respect to the Mandatory Change or as may otherwise be agreed to by the Parties in writing or determined in the settlement of a Dispute in accordance with paragraph (d)(iii) above; and

(f) the Parties will cause a record of each Mandatory Change and Mandatory Change Request to be maintained as contemplated in Section 7.12 (*Record of Changes*).

7.9 Change Orders.

A Change Request or a Mandatory Change Request will become a "**Change Order**" when the requirements of the procedures to consider such Change Request or Mandatory Change Request set out in this Article 7 (*Change Order Process*) have been satisfied, and the Change Request or Mandatory Change Request is Approved by each of the Parties, where such Approval is required pursuant to this Article 7 (*Change Order Process*).

7.10 Implementation of Change Orders.

The Service Provider will minimize disruption to the delivery of the Services and to the business operations of the Province and the Stakeholders as the result of the implementation of a Change Order arising from a Change Request or a Mandatory Change Request. The cost of implementing a Change Order will be borne as set out in the Change Order or as otherwise provided in this Agreement. All privacy reviews contemplated in **Schedule 24** *(Privacy Obligations)* will be conducted in respect of any Change Order as more specifically set forth in **Schedule 24** *(Privacy Obligations)*.

7.11 Consequential Amendments.

If the Parties proceed with a Change Order (whether as the result of a Change Request or a Mandatory Change Request), then the Change Order will constitute an amendment to this Agreement including the relevant Schedules to this Agreement. From and after the effective date of the implementation of a Change Order, this Agreement will be interpreted as amended by the Change Order, and this Agreement, as so amended, will continue in full force and effect for the remainder of the Term.

7.12 Record of Changes.

The Parties will jointly maintain an accurate and complete record of all changes to the Services contemplated in this Article 7 (*Change Order Process*) including all Ordinary Course Changes, Change Requests, Mandatory Change Requests, Mandatory Changes and Change Orders. Such record may be maintained in such form as the Parties may agree pursuant to the Governance Process, including by way of a server-based record accessible by both Parties. Each Party will cooperate to make corrections to such records as the other Party may reasonably request to ensure that the record of all changes is accurate and complete, in all material respects, at all times throughout the Term.

ARTICLE 8 – SERVICE LEVELS

8.1 Overview of Service Levels.

Subject to the specific and more detailed provisions of this Article 8 (*Service Levels*), and any higher standard or level of performance otherwise required in this Agreement which may be applicable in the circumstances, the Service Provider will perform the Services throughout the Term to a standard and level of performance which:

(a) is equal to, or greater than, the standard and level of performance for such Services immediately before the Hand-Over Date; and

(b) will maintain or increase the satisfaction of the customers of the Services, the Province and Stakeholders.

For greater clarification, the provisions of this Section will apply to all of the Services, including those portions of the Services that are not specifically measured or otherwise monitored through the use of Service Levels.

8.2 General Compliance.

The Parties acknowledge and agree that:

(a) the Service Provider will perform the Services throughout the Term to a standard and level of performance which is required in order for the Service Provider to meet or exceed the Service Levels;

(b) the Service Levels set out in this Agreement, as may be amended from time to time in accordance with this Agreement, are intended to be baseline performance standards and levels for the delivery and performance of the Services;

(c) during the Term, the Service Provider will identify ways to improve or increase the Achieved Service Levels including, without limitation, continually monitoring and evaluating changes and trends in the **[insert relevant industry]** field of operations and monitoring and evaluating new and available technologies and service delivery processes and strategies that are applicable to the Services;

(d) during the Term, the Service Provider will use commercially reasonable efforts to continually improve the quality of the Services and the Achieved Service Levels in a manner consistent with the terms and intent of this Agreement, taking into account the cost of such improvement as compared to the benefit to be derived therefrom; and

(e) any improvements in the Achieved Service Levels or performance standards and levels achieved by the Service Provider in providing the Services, whether or not as part of any progressive improvement requirements contemplated in this Agreement, will not result in an increase in the Fees payable under this Agreement unless otherwise Approved by the Province.

8.3 Transformed Service Levels.

With respect to any Service Levels for the Transformed Services, such Service Levels will only apply after the Acceptance Date for the Stage applicable to such Transformed Services.

8.4 Restrictions on Changes to Service Levels.

The Service Provider acknowledges that the establishment of Service Levels is a matter of fundamental importance for the Province. The Service Provider will not agree or purport to agree with any Stakeholder or other Person, whether in its own right or purportedly as agent for and on behalf of the Province, to amend, change or modify in any manner any of the Service Levels without the Approval of the Province.

8.5 Review and Changes to Service Levels.

The Parties acknowledge and agree that Service Levels are intended to be comprehensive, but not all inclusive, and accordingly, it is the intention of the Parties that during the Term the Parties may agree to different or additional Service Levels in respect of any of the Services. On an annual basis during the Term, and pursuant to the Governance Process, the Parties will jointly review the following:

(a) the then-current Service Levels;

(b) generally available information indicating industry-wide improvements in delivery of substantially similar services (including any available Benchmarker's reports commissioned in accordance with Article 9 (*Benchmarking*)); and

(c) improved performance capabilities, including those associated with advances in technology and processes used to provide the Services.

On the basis of such review, the Parties will discuss and agree upon whether any of the Service Levels will be adjusted. Any such adjustment will be subject to the mutual agreement of the Parties in accordance with the Governance Process, or as a Change Order through the Change Order Process. Any such adjustments, whether agreed to by the Parties in writing and signed by both Parties through the Governance Process, or whether through a Change Order pursuant to the Change Order Process, will be and be deemed to be an amendment to the Service Levels contained in **Schedule 11** *(Service Levels)* of this Agreement.

8.6 Monitoring.

From and after the Hand-Over Date, the Service Provider will establish and maintain in place, at all times, appropriate policies and procedures to monitor and evaluate the achievement of the Service Levels during the applicable measurement periods, including the maintenance of a service level log in order to permit the Service Provider, and the Province (as applicable), to:

(a) evaluate Achieved Service Levels;

(b) satisfy the reporting obligations under this Agreement;

(c) respond to, or to assist the Province in responding to, inquires from Stakeholders, the Ministry or any customers of the Services regarding the Service Provider's performance of the Services;

(d) enable the Province to report publicly on the achievement or non-achievement of the Service Levels by the Service Provider in accordance with the Province's Policy, as such Policy may be amended from time to time; and

(e) confirm and verify Achieved Service Levels in respect of any Service Level from time to time upon reasonable notice.

8.7 Service Level Reports.

From and after the Hand-Over Date, and without limiting the application of Section 8.6 *(Monitoring)*, the Service Provider will prepare and maintain records and reports summarizing its Achieved Services Levels and providing the particulars of any failure of the Service Provider to meet a Service Level, organized by Service type (to the extent possible) and in such form and content as the Province may require. For greater clarification, any reports regarding the failure of the Service Provider to meet a Service Level will include detail regarding the particulars of the failure, a description of the measures taken or to be taken by the Service Provider to rectify and remedy the failure, and the timeline in which such measures were or are expected to be taken by the Service Provider, in order to allow the Province to:

(a) evaluate the consequence of such failure;

(b) communicate with or respond to the applicable Province customers or Stakeholders that received the Service that failed to meet such Service Level; and

(c) cooperate with the Service Provider to rectify and remedy the consequence of such failure and to prevent future failures to meet such Service Level.

The Service Provider will provide such reports to the Province on a monthly basis and in accordance with applicable reporting requirements set out in **Schedule 21** *(Reporting Requirements)*, unless sooner requested by the Province from time to time. The Service Provider will also provide the Province with immediate notice of each material failure to meet a Service Level in accordance with the provisions of Section 8.8 (*Problem Alert and Escalation Procedures*).

8.8 Problem Alert and Escalation Procedures.

In order to facilitate the ability of the Parties to quickly address, mitigate or otherwise deal with an event, occurrence, error, deficiency, defect, interruption, malfunction or other similar matter with respect to the Services, or any other System or service provided by a Subcontractor or any other Person which is related to or otherwise impacts the Services, and which the Service Provider reasonably believes could have a material adverse effect on the delivery of the Services or could result in the Service Provider failing to meet a Service Level (each a "**Problem**"), the following provisions will apply:

(a) from and after the Hand-Over Date, the Service Provider will develop, implement, maintain and comply with Problem alert, escalation, and management procedures, which may be amended by the Parties through the Governance Process from time to time (the "**Problem Management Procedures**");

(b) if the Service Provider becomes aware of a Problem, then the Service Provider will immediately notify the Province of the Problem or, to the extent that such immediate notice is not possible, as soon as possible, by providing the Province with the particulars of the Problem;

(c) the Service Provider will treat the Problem as a priority, will work diligently to avert or minimize any adverse effect that the Problem may cause, and will deal with the Problem in accordance with the Problem Management Procedures;

(d) upon the occurrence of any Problem, the Service Provider will perform a root cause analysis in respect thereof as soon as practicable, and in any event, within any times required pursuant to the Problem Management Procedures, for purposes of identifying the cause of such Problem, and in order to assist the Service Provider in developing and implementing a proposal or workaround solution for correcting the Problem, and implementing improved processes to detect and avoid similar Problems in the future;

(e) the root cause analysis and proposal will be completed by the Service Provider as part of the Services at no additional cost to the Province;

(f) for greater clarification, and for purposes of this Section, any Problems of Subcontractors and Suppliers will be deemed to be Problems of the Service Provider; and

(g) the Service Provider will review each root cause analysis with the Province, monthly (or more frequently as may be requested by the Province from time to time) to monitor Service Provider's corrective and remedial actions (including detective and preventive actions).

For greater certainty, the Service Provide will not be required to perform a root cause analysis as described in Subsections 8.8(d), 8.8(e) and 8.8(g), in connection with a Problem in reqpest of systems owned or controlled by third parties (other than Subcontractors and Suppliers) for which the Service Provider has no control.

8.9 Service Level Failures.

The Service Provider's failure to meet any Service Level Requirement will be governed by the provisions of **Schedule 12** (*Service Level Failures*). The provisions of **Schedule 12** (*Service Level Failures*) provide only partial compensation for the damage that may be suffered by the Province as a result of the Service Provider's failure to meet any Service Level Requirement. Accordingly, payment or application of any Service Level Credit pursuant to the provisions of **Schedule 12** (*Service Level Failures*) is without prejudice to any entitlement that the Province may have to damages or other remedies under this Agreement, at law or in equity, including injunctive relief (to the extent available), as well as to the following:

(a) the removal of the Service in respect of which there was a failure to meet the applicable Service Level Requirement from the Services to be provided by the Service Provider pursuant to this Agreement, and an appropriate consequential reduction in the applicable portion of the Fees pursuant to the Change Order Process;

(b) the taking by the Province of all action necessary or desirable to correct, rectify and remedy such failure and the resulting consequences at the cost of the Service Provider including, without limitation, procuring or otherwise obtaining Services or goods from any alternative service providers or suppliers, and setting-off the cost of all such action and of the amount of all damages or loss suffered by the Province as a result of such failure against the Fees otherwise payable by the Province to the Service Provider; or

(c) a claim by the Province against the Guarantors under the Guarantees.

A failure to meet a Service Level Requirement which does not give rise to a Service Level Termination Event will not give rise to a right of the Province to terminate this Agreement, but will give rise to rights and remedies of the Province in respect of defaults generally in accordance with this Agreement including, without limitation, the provisions of this Section and the right to Service Level Credits in accordance with the provisions of **Schedule 12** (*Service Level Failures*).

ARTICLE 9 – BENCHMARKING

9.1 Benchmarking.

The Province may require benchmarking comparisons of any one or more of the Fees or the Service Levels to be performed (each, a "**Benchmarking**"), in which case the following will apply:

(a) the Benchmarking will not be performed more frequently than **[insert frequency number]** in any **[insert applicable number]** consecutive Contract Years, and the first Benchmarking will not be performed before **[insert date]**;

(b) the Service Provider will cooperate with the Province in connection with any such Benchmarking in the manner contemplated in Section 9.2 (*Benchmarking Cooperation*);

(c) the third party consultant performing the Benchmarking (the "**Benchmarker**") will be selected and engaged by the Province and the Service Provider jointly. If the Province

and the Service Provider are not able to agree on the selection of the Benchmarker, then the matter will be a Dispute and will be settled in accordance with Article 27 *(Dispute Resolution)*;

(d) except as set forth in paragraph (g) below, the costs of the Benchmarker will be shared equally between the Province and the Service Provider;

(e) as a condition to its engagement, the Benchmarker will execute a Non-Disclosure Agreement;

(f) the Benchmarking will be a comparison of any one or more of the Service Levels and the Fees with the same or similar comparators of other entities receiving similar services, with appropriate adjustments being made where quantities or circumstances differ; and

(g) the Province will be entitled to perform one (1) Benchmarking at any time after the Province gives notice, or is deemed to have given notice, to the Service Provider under Sections 2.5 (*Renewal Notice*) or 2.6 (*Renewal Negotiations*) that the Province does not intend to renew this Agreement, at the sole cost of the Province.

9.2 Benchmarking Cooperation.

Unless the Parties otherwise agree, the Province will, with the Service Provider's concurrence, determine the scope, methodology, relative comparisons and execution of each Benchmarking. The Service Provider will cooperate in the Benchmarking studies by providing information requested in relation to the Benchmarking, and in particular, the Service Provider will provide:

(a) the Benchmarker (and will ensure that its Subcontractors provide, either directly to the Benchmarker or to the Service Provider), all necessary information, documents and assistance as may be reasonably required for the Benchmarker to perform the Benchmarking; and

(b) the Benchmarker with reasonable access to the Service Provider's performance data and, where necessary, access (which may be supervised) to the Service Provider's performance measurement tools to independently verify reported Achieved Service Levels.

9.3 Benchmarker's Report.

Each Party will receive a copy of the Benchmarker's report and will have an opportunity to review the same and make submissions to the other Party with respect to the findings contained in the Benchmarker's report prior to any adjustments to the Services, the Service Levels or the Fees as a result of such Benchmarking. Any such adjustments will be subject to the mutual written agreement signed by the Parties in accordance with the Governance Process or through the Change Order Process, as applicable. If the Benchmarking results show that the Service Levels reported by the Service Provider are materially different than actual performance, then the Benchmarker will use actual performance as the basis of comparison.

9.4 Customer Satisfaction.

The Service Provider will cooperate with the Province to obtain information concerning the levels of Stakeholder and customer satisfaction with the Services, including by the following:

(a) assisting the Province to survey Stakeholders and customers as to their level of satisfaction with the performance of the Services, which surveys will be initiated and undertaken by the Service Provider only upon the direction and Approval of the Province (and the Approval of the Province will include Approval as to the format, content and process for such survey to be conducted by the Service Provider); and

(b) tracking performance levels and customer complaints as well as the response to and handling of such complaints.

The results of any customer satisfaction surveys will be reviewed by the Parties through the Governance Process. If the results of the survey indicate a failure or perceived failure to meet applicable Service Levels, or a decrease in the level of customer satisfaction, then within two (2) months of receipt of the survey results, the Service Provider will design and propose a remedial plan (in consultation with the Province through the Governance Process) to prevent reoccurrence of the problem and to increase customer satisfaction of the applicable parties. The Service Provider will implement the same in accordance with the Change Order Process.

ARTICLE 10 – BRANDING AND COMMUNICATIONS

10.1 Province Marks.

[NOTE – use of Province Marks by the Service Provider will require consent from the Province's Public Affairs Bureau] In respect of the use or display by the Service Provider of any trade-marks, official marks, business names, trade names, domain names, trading styles, logos, or other distinguishing marks of the Province, whether registered or unregistered (each a "**Province Mark**"), the Parties agree as follows:

(a) prior to any display or use of a Province Mark by the Service Provider in the performance of the Services, the Service Provider will obtain the Approval of the Province;

(b) subject to Section 10.2 (*Brand Use*), any display or use of the Province Marks by the Service Provider will only be for the duration of the Term, on a non-exclusive basis, and only for the purposes of providing the Services;

(c) the Service Provider will use the Province Marks only in accordance with this Agreement and in the manner expressly permitted in writing by the Province and provided that:

(i) the character and standards of quality of the wares and Services in respect of which the Province Marks may be used by the Service Provider are as set out in **Schedule 15** *(Conditions of Use of Province Marks)*,

(ii) such display or use of the Province Marks is in accordance with the provisions of **Schedule 15** *(Conditions of Use of Province Marks)*, appropriate legends and the Province Policies including, without limitation, any policies established or enforced by the Province's Public Affairs Bureau, notice of which will be given to the Service Provider, and all usage guidelines and restrictions as reasonably prescribed from time to time by the Province in respect thereof, or in accordance with other express permissions granted by the Province, and

(iii) the Service Provider may not register or carry on business under a business name that contains any of the Province Marks unless specifically Approved by the Province;

(d) upon Termination of this Agreement, the Service Provider:

(i) will immediately cease any and all use of the Province Marks,

(ii) will discontinue the provision of all products and Services in association with the Province Marks, and

(iii) will not, and will ensure that its Affiliates do not, thereafter use the Province Marks or any trade-mark or trade name confusingly similar to the Province Marks;

(e) during and after the Term the Service Provider will not, and will ensure that its Affiliates do not, challenge the validity of the Province Marks or the Province's ownership of the Province Marks;

(f) any and all goodwill that is or may be acquired from the use of a Province Marks by the Service Provider or its Affiliates will vest in and be, and be deemed to be, the property of the Province;

(g) the Province is and will remain the owner of the Province Marks, and the Service Provider will not obtain any rights in or to the Province Marks other than the right to use the Province Marks in accordance with the provisions of this Section 10.1 (*Province Marks*);

(h) at the request of the Province, the Service Provider will provide the Province with samples of the Service Provider's use of the Province Marks; and

(i) the Service Provider will not use or register any Province Marks or any marks confusingly similar to the Province Marks except as expressly Approved by the Province under or in accordance with the terms of this Agreement.

10.2 Brand Use.

The Service Provider will provide the Services under the branding of the Province Marks set forth in **Schedule 15** *(Conditions of Use of Province Marks)*, but subject to the provisions of Section 10.1 (*Province Marks*), as the same may be changed from time to time by the Province pursuant to the Change Order Process, all of which is hereby Approved by the Province. Such Approval by the Province will not restrict the Province's right to use any such Province Marks, or to license the same to any other Person, or use or license any other Province Marks similar thereto.

10.3 Service Provider Marks.

Except as may otherwise be expressly required pursuant to Applicable Law, or as may be Approved by the Province, the Service Provider will not use or display any of the Service Provider's trade-marks, official marks, corporate names, business names, trade names, domain names, trading styles, logos, or other distinguishing marks (each a "**Service Provider Mark**") together or in conjunction with any Province Marks. Notwithstanding any such requirement pursuant to Applicable Law, or Approval by the Province, the Province will not obtain any rights in or to the Service Provider Marks, and any and all goodwill that is or may be acquired from the such use of a Service Provider Mark by the Service Provider will vest in and be, and be deemed to be, the property of the Service Provider.

10.4 Publicity.

The Service Provider will submit to the Province all advertising, written sales promotion, press releases, public notices and any and all other publicity matters or materials relating to this Agreement or the transactions contemplated by this Agreement, or in which the Province's name or any Province Marks are mentioned or language from which connection with the Province's name or any Province Marks may be inferred or implied (the "**Publicity Materials**"). The Service Provider will not publish or use any Publicity Materials without the prior consultation with and Approval of the Province, which Approval will not be unreasonably withheld. Notwithstanding the foregoing, the Service Provider may include the Province's name and a factual description of the work performed under this Agreement only:

(a) on employee bulletin boards;

(b) in internal business planning documents;

(c) for account referral purposes when Approved by the Province;

(d) whenever otherwise required by reason of legal, accounting or regulatory requirements; and

(e) in proposals where such proposal language has been Approved by the Province.

In addition, no disclosure, including press releases, will be made by the Service Provider regarding any aspect of the Services or the Province without the Approval of the Province. In the event of potentially negative publicity or other potentially adverse effects upon the Service Provider in connection with the Services or this Agreement, the Service Provider will be entitled to respond to the same provided that it does so in consultation with the Province, and that the Province is given the opportunity to first Approve the contents of any such response insofar as it relates to the Province, the Services or this Agreement.

10.5 Stakeholder Communications.

Unless specifically provided otherwise in this Agreement, all communications by the Service Provider to the Stakeholders will be in accordance with the Communication Plan and other processes and procedures as set forth in **Schedule 17** *(Communications Plan and Processes)*.

10.6 Adverse Impact Notice.

The Service Provider will provide the Province with prior notice (which need not be in writing), if possible, of events with respect to the Service Provider and its Affiliates that the Service Provider anticipates will become public and could reasonably be expected to adversely impact the Province or the relationship between the Parties, or be covered negatively in any North American media. The Service Provider's obligation to provide such notice is subject to the provisions of applicable law, including securities laws applicable to the Service Provider and its Affiliates, and to the confidentiality obligations of the Service Provider and its Affiliates. Where it is not possible for the Service Provider to provide prior notice to the Province, the Service Provider will notify the Province as soon as possible.

ARTICLE 11 – RELATIONSHIP MANAGEMENT AND HUMAN RESOURCES

11.1 Governance.

During the Term, the relationship of the Parties (including the mechanisms by which they will manage this Agreement, each with the other) will be expressly governed by the provisions of this Article 11

(*Relationship Management and Human Resources*) and the processes, procedures and provisions set forth in the governance structure attached as **Schedule 18** *(Governance)*, as **Schedule 18** *(Governance)* may be jointly amended from time to time by the Parties in accordance with the terms of this Agreement.

11.2 Cooperation of the Parties.

Each Party will cooperate with the other, in good faith, in the performance of its obligations under this Agreement. In connection therewith, each Party will make available, as reasonably requested by the other Party, such management decisions, information, approvals and acceptances such that the provision of the Services under this Agreement may be accomplished in a proper, timely and efficient manner and in accordance with the processes and procedures set forth in this Agreement. Unless specifically provided otherwise in this Agreement, where an agreement, approval, acceptance or consent of the other Party is required by any provision of this Agreement, then such action will not be unreasonably withheld or delayed, having regard to all of the surrounding circumstances. The Parties agree that it will not be considered reasonable for any requested response time for an agreement, approval, acceptance or consent from the Province to be less than five (5) Business Days except in extraordinary circumstances clearly demonstrated in writing by the Service Provider. Notwithstanding the foregoing, nothing in this Section 11.2 (*Cooperation of the Parties*) will in any manner relieve the Service Provider from performing its obligations, or delivering the Services, as contemplated under, and in accordance with, the express terms of this Agreement.

11.3 Power and Authority of the Service Provider.

Except as otherwise set forth in this Agreement, and subject to the terms of this Agreement, the Service Provider will have the power and authority to take such actions as it deems to be prudent, necessary or advisable to perform the Services in accordance with the terms and conditions set forth in this Agreement. Notwithstanding the foregoing, the Service Provider will not take any action required by this Agreement, if such action is:

(a) subject to the Approval of the Province, without having received such Approval; and

(b) subject to consultation with the Province, without having undertaken such consultation.

For greater clarification, no such Approval or consultation will in any manner relieve the Service Provider from performing its obligations, or delivering the Services, as contemplated under, and in accordance with, the express terms of this Agreement, nor will such Approval or consultation have any effect on the allocation of risk to the Service Provider as a result of the covenants, obligations and requirements of the Service Provider under the terms of this Agreement.

11.4 Province's Right to Issue Directives.

The Province may, from time to time, at the Service Provider's request or at the Province's own initiative, issue written directives and instructions and establish written policies and procedures governing the duties and obligations of the Service Provider relating to the Services (including with respect to confidentiality, privacy and security), in order to cause the Service Provider to comply with the Province's Policies or business requirements in the performance of the Services (each a "**Directive**"), in which case, the following provisions will apply:

(a) the Directives will be subject to the Change Order Process and will be deemed to be a Mandatory Change Request;

(b) the Province will, through the Governance Process, provide the Service Provider with timely written notice of the Directives;

(c) the Service Provider will at all times act in accordance with the Directives that it has so received from the Province, provided that the Directives do not oblige the Service Provider to perform any duty or obligation not provided for or otherwise contemplated under this Agreement, and do not have the effect of causing the Service Provider to be in breach of any Applicable Laws;

(d) the Province will provide the Service Provider with a reasonable period of time to comply with a Directive, having regard to all of the surrounding circumstances, the nature of the Directive, and the requirements of the Change Order Process (including, without limitation, the Mandatory Changes), it being acknowledged by the Parties that the nature of some Directives may necessitate immediate compliance, in which case, the Service Provider will comply with the Directive as promptly as practicable; and

(e) subject to the requirements of the Change Order Process (including, without limitation, the Mandatory Changes), the failure or refusal of the Service Provider to comply with a Directives that it has received from the Province within the times required pursuant to this Agreement, and in accordance with the provisions of this Section, may constitute a Material Breach under the provisions of Section 28.1 *(Service Provider Material Breach)*.

11.5 Province Approval.

In connection with the Services performed by the Service Provider under this Agreement, and unless specifically provided otherwise in this Agreement, the Service Provider will not undertake any matter outside of the scope of the Services contemplated under this Agreement throughout the Term, and will not undertake any of the following matters without the prior Approval of the Province:

(a) any financing or borrowing from a Person other than from an Affiliate of the Service Provider, and other than trade credit in the ordinary course, that could cause or permit (and the Service Provider will not otherwise cause or permit) the creation or maintenance of any security interest, charge, pledge or other encumbrance on the rights of the Service Provider under this Agreement or on any assets used in the provision of Services by the Service Provider or its Affiliates (other than leased equipment from arm's length third parties);

(b) those matters specifically identified in this Agreement as requiring the Approval or other authorization or consent of the Province;

(c) making or agreeing to make any capital expenditure on behalf of the Province; or

(d) retaining legal counsel on behalf of the Province with respect to any matter involving any Service, or initiating or responding to any legal, regulatory or other proceeding on behalf of the Province, or settling any Claim prosecuted by or against the Province arising from a legal or regulatory proceeding regarding any Service.

If the Approval of the Province is required pursuant to this Agreement, then except as specifically provided otherwise in this Agreement, the Service Provider will deliver written notice to the Province through the Governance Process, setting out the particulars of the matter and requesting the Approval of the Province, and setting forth the reasonable time period in which a response is required, and if

applicable, the implications of not responding within that time period. The Parties agree that it will not be considered reasonable for the requested response time to be less than five (5) Business Days except in extraordinary circumstances clearly demonstrated in the Service Provider's notice. The Province will use reasonable efforts to respond to any request from the Service Provider for the Approval of the Province within a reasonable period of time, having regard to all of the surrounding circumstances. Except as specifically provided otherwise in this Agreement, the failure of the Province to respond to a request for an Approval during the period suggested by the Service Provider will not result in any liability on the part of the Province to the Service Provider or be deemed to constitute the Approval of the Province by acquiescence or otherwise. Where the Province delays in providing such response to the Service Provider in circumstances where the request for the Approval from the Service Provider expressly sets forth the consequences of not responding within the required time period, then the Service Provider will not be responsible for any breach by the Service Provider of its obligations under this Agreement where the same are directly attributable to the delay of the Province in providing such response.

11.6 Key Positions.

Recognizing the importance of executive continuity to the ongoing success of the Parties' relationship, and to the successful performance of the Services under this Agreement, the Service Provider will use all reasonable efforts to minimize turnover of personnel in the Service Provider positions, as more particularly described in **Schedule 19** *(Key Positions)* (the "**Key Positions**"), as may be changed from time to time by the Parties in accordance with this Section 11.6 (*Key Positions*) and Section 11.7 (*Changes in Key Positions*). At all times during the Term, the Service Provider will ensure that the Key Positions are appropriately staffed and available as may be necessary to ensure the continuous and uninterrupted provision of the Services. Subject to Subsection 11.7(a) and (b) (*Changes Key Positions*), the foregoing will constitute a material obligation for purposes of Section 28.1 *(Service Provider Material Breach)*. The Parties may, from time to time through the Governance Process, re-designate the positions that constitute Key Positions.

11.7 Changes in Key Positions.

The Province has entered into this Agreement in reliance upon and with the expectation that the personnel in the Key Positions will be engaged in the provision of the Services to the Province, and with the expectation of reasonable continuity in the Key Positions. Accordingly, the Service Provider will implement personnel changes in the Key Positions in accordance with the following:

(a) the Service Provider may replace a person holding a Key Position, or appoint a new person to fill a vacancy caused by the resignation or other departure of a person holding a Key Position, provided that:

(i) the Service Provider does not transfer any individual in Key Position on a lateral basis without promotion to another project or Affiliate of the Service Provider without the prior Approval of the Province,

(ii) the Service Provider provides the Province with reasonable prior written notice thereof, if possible, together with relevant information regarding the background qualifications of the person that the Service Provider wishes to appoint to the Key Position, and such other information regarding the qualifications of such person as the Province may request,

(iii) the Service Provider provides the Province with the opportunity to interview the person that the Service Provider wishes to appoint or hire into the Key Position prior to the final decision being made in respect of such appointment or hire, and

the Service Provider considers comments from, and consults with, the Province in respect of such interview,

(iv) the Service Provider obtains the Approval of the Province pursuant to the provisions of **Schedule 19** *(Key Positions)* in respect of any candidate that will replace **[insert critical key positions, e.g., President, Operational VP, etc.]** of the Service Provider, and

(v) the Service Provider provides the Province with a transition plan for the replacement of the incumbent with a new person in the Key Position;

(b) in the event of an extended or unexpected absence of the incumbent in a Key Position, the Service Provider will forthwith advise the Province of such absence, and the Parties will consult with each other as to the appropriate steps to be taken by the Service Provider in respect of such absence; and

(c) any person assigned to or otherwise placed in a Key Position will have qualifications or experience appropriate to the position which will be at least equivalent to the qualifications and experience of the initial person in such Key Position unless otherwise Approved by the Province, and such person will be suitably trained and transitioned to the Key Position.

11.8 Key Position Failures.

At any time, and from time to time, during the Term, the Province or the Service Provider may by notice (which may be oral) to the other, declare that a Key Position has failed to satisfactorily perform the duties of such position. The parties will promptly discuss such concerns, and where the Parties cannot agree on an appropriate course of action in respect thereof, then such issue will be elevated to the **[Joint Executive Committee]** for consideration, or such other discreet channels of communication as may be appropriate under the circumstances. Where the **[Joint Executive Committee]** provides any direction, including removal of such person, then the Service Provider will promptly adhere to and implement such direction at the Service Provider's sole cost.

11.9 General Principles Regarding Personnel.

At all times during the Term, the Service Provider will employ sufficient personnel of the Service Provider, including both employees and independent contractors of the Service Provider (collectively, "**Personnel**"), and will ensure that sufficient personnel is employed by its Subcontractors (collectively, "**External Personnel**"), to perform the Services in accordance with Service Levels and the other terms and conditions of this Agreement. The following provisions will apply with respect to the Personnel and the External Personnel:

(a) unless specifically provided otherwise in this Agreement, the Service Provider will be responsible for the management and supervision of, and for the acts, omissions, performance of, and damage caused by the Personnel and External Personnel in the performance of the Services;

(b) the Service Provider will ensure that the use of all Foreign Employed Individuals in the performance of the Services will comply with the Privacy Obligations applicable thereto;

(c) the Service Provider will ensure that the Personnel and External Personnel performing the Services:

(i) possess a degree of skill and experience appropriate to the tasks to which they are assigned and the performance and Service Levels which they are required to achieve,

(ii) receive appropriate training (including quality training courses, refresher courses and retraining programs) for the performance of the Services and compliance with the confidentiality provisions and Privacy Obligations in the Agreement,

(iii) perform the Services to the standards set out in this Agreement, and

(iv) strictly comply with the privacy, security and confidentiality provisions set forth in the Privacy Obligations;

(d) where given a Directive by the Province pursuant to Section 11.4 (*Province's Right to Issue Directives*), or where otherwise necessary, appropriate or prudent to do so given the nature of the Services or of the Province Confidential Information being accessed, used or disclosed, the Service Provider will conduct appropriate background checks with respect to the applicable Personnel, and will contractually require Subcontractors to do the same with respect to the applicable External Personnel, prior to such personnel commencing to provide the Services;

(e) subject to the terms of the Master Transfer Agreement and unless specifically provided otherwise under this Agreement, the Service Provider will be solely liable and responsible (to the exclusion of the Province) for all costs, expenses, liabilities or claims, whenever incurred, relating to:

(i) salaries and other compensation payable to its Personnel,

(ii) labour relations proceedings or orders, grievances, arbitration proceedings or unsatisfied arbitration awards relating to its Personnel,

(iii) strikes or other actions due to labour disputes involving its Personnel, and

(iv) complaints, claims, decisions, applications, orders or prosecutions under any employment or labour standards, occupational health and safety, workers' compensation, pay equity, employment equity and human rights legislation relating to its Personnel,

regardless of the time that the matter or event giving rise to any such costs, expenses, liability or claims arises or occurs, and for greater clarification, unless provided otherwise under the terms of the Master Transfer Agreement or this Agreement, none of such costs, expenses, liabilities or claims referred to in this paragraph (e) above will be subject to reimbursement by the Province to the Service Provider;

(f) the Service Provider will deal with its Subcontractors in such a manner that the Province will have no liability resulting from the failure of the Subcontractors to meet the same responsibilities and payment obligations as described in paragraph (e) above with respect to the External Personnel, and for greater clarification, none of such costs, expenses, liabilities or claims contemplated in this paragraph (f) will be subject to reimbursement by the Province to the Service Provider or to the Subcontractors;

(g) the Service Provider will comply at all times with all applicable collective agreements and all applicable employment standards, occupational health and safety, workers' compensation, human rights legislation, and other Applicable Laws relating to its Personnel, will cause each Subcontractor to comply with the same as applicable to the External Personnel of such entities, and will deal with all Subcontractors in such a manner that the Province will have no liability resulting from any failure of the Subcontractors to so comply with such responsibilities and obligations with respect to the External Personnel; and

(h) except as expressly provided otherwise in this Agreement or in the Master Transfer Agreement, the Service Provider will be solely liable and responsible for, to the exclusion of the Province, all costs arising from or otherwise relating to the termination by the Service Provider of any Personnel, and will ensure that the Province has no liability for the termination by any Subcontractor of any External Personnel, and the Service Provider and the Subcontractors will not be reimbursed by the Province for any such costs, expenses, claims or liabilities.

11.10 Administrator.

The Province shall act as the administrator of the Agreement, appointed by the Broader Public Sector, in connection with the Broader Public Sector's purchase of Services.

ARTICLE 12 – SUBCONTRACTORS

12.1 Responsibility for Subcontractors.

The Service Provider is the general contractor for the Services under this Agreement and remains responsible for all of its obligations under this Agreement, regardless of whether the Service Provider relies upon any Subcontractor to any extent. Subject to the terms of this Agreement:

(a) the Service Provider's use of Subcontractors for any of the Services will in no way increase the Service Provider's rights or diminish the Service Provider's liabilities to the Province with respect to this Agreement;

(b) the Service Provider's rights and liabilities under this Agreement with respect to the Province will be as though the Service Provider had itself performed such Services;

(c) the Service Provider will be liable for any defaults or delays caused by any Subcontractor in connection with the Services as if such defaults or delays were caused by the Service Provider; and

(d) the Service Provider will be fully liable for all actions and omissions of the Subcontractors in the performance of the Services.

If a Subcontractor breaches a Subcontract, or is alleged to have breached a Subcontract, which could have a material affect on the delivery of the Services or the performance of the Service Provider's obligations under this Agreement, then the Service Provider will notify the Province in writing and provide the Province with such information relating to the alleged breach as the Province may request.

12.2 Inconsistent Subcontract Terms.

The terms of this Agreement will in all events be binding upon the Service Provider notwithstanding, and without regard to, the existence of any inconsistent or contrary terms in any agreement between the Service Provider and any Subcontractor, whether or not and without regard to the fact that the Province may have directly or indirectly been given or otherwise received notice of any such inconsistent or contrary term.

12.3 General Contract Terms (Subcontractors).

Subject to Section 12.8 (*Material Subcontractors*), all Subcontracts entered into by the Service Provider with Subcontractors will not include any terms or provisions that are inconsistent with, or contrary to, the terms and conditions of this Agreement, and all such Subcontracts will include the following provisions:

(a) a requirement that the Subcontractor adhere to the applicable obligations that:

(i) are expressly required by this Agreement to be imposed upon the Subcontractor, and

(ii) are otherwise required for the Service Provider to perform its obligations to the Province under this Agreement including, without limitation, the Service Levels, confidentiality obligations, intellectual property provisions, Privacy Obligations, and reporting, audit and access rights and requirements;

(b) assignment or licensing of Intellectual Property Rights to the Service Provider in respect of any deliverables created in such relationship, and waiver of moral rights in respect of the same, to the extent required by the Service Provider to comply with its obligations to the Province under this Agreement;

(c) obligations regarding compliance with Applicable Laws, including source deductions and remittances (for taxes, workers compensation and similar requirements);

(d) termination rights consistent with the terms of this Agreement;

(e) to the extent possible, assignment rights to the Province or the Alternative Service Provider upon the early termination or expiry of this Agreement in accordance with its terms, without any further consent from the Subcontractor or any additional, accelerated or other similar payments having to be made; and

(f) any other provisions necessary for the Service Provider to fulfill its obligations under this Agreement.

The foregoing will not apply with respect to any Assigned Contracts to the extent set forth in Section 12.7 (*Assigned Contracts*).

12.4 Subcontractor Monitoring.

During the Term, the Service Provider will:

(a) monitor the performance of Subcontractors and promptly address and remedy any performance issues or disputes with Subcontractors in such a manner as to mitigate any adverse impact on the nature, quality or delivery of the applicable Services;

(b) address and remedy any performance issues or disputes with Subcontractors in a manner which has no adverse impact on the nature, quality or delivery of the applicable Services under this Agreement; and

(c) ensure that contingency plans are devised for the possibility of a Subcontractor failing to perform, needing to be replaced, or terminating the Subcontract with the Service Provider before the Termination of this Agreement.

12.5 Non-Disclosure Documents.

Unless otherwise Approved by the Province, all External Personnel of Access Subcontractors (including all External Personnel of any Affiliates of the Service Provider who may have access to, or use or disclosure of, Personal Information) will be required to execute documents directly with the Province binding such External Personnel to confidentiality and non-disclosure agreements as required by the Province and in a form Approved by the Province, all as more particularly described in the Privacy Obligations contained in **Schedule 24** *(Privacy Obligations)* (the "**External Personnel Agreements**"). The Service Provider will not disclose or provide access to any Personal Information to any such External Personnel until such External Personnel have entered into an External Personnel Agreement.

12.6 Confidentiality Breaches.

Unless specifically provided otherwise under this Agreement, any breach of the confidentiality obligations set forth in this Agreement by a Subcontractor, or any External Personnel of such Subcontractor, will be deemed to constitute a breach of the confidentiality provisions of this Agreement by the Service Provider. In the event of any breach of confidentiality obligations by a Subcontractor, or any External Personnel of a Subcontractor, the Parties agree as follows:

(a) in the event that either Party discovers that a breach of confidentiality by a Subcontractor or any External Personnel of a Subcontractor has occurred, it will promptly notify the other Party in writing;

(b) the Service Provider will take all steps necessary to remedy or to have remedied such breach;

(c) the Service Provider will develop and inform the Province of any remedial plans to remedy or otherwise deal with such breach;

(d) if the Province Approves such remedial plan, and the Service Provider carries out the remedial plan, then the Province will not be entitled to terminate this Agreement solely on the basis of the Subcontractor's breach of confidentiality;

(e) if the Service Provider does not carry out the remedial plan, then such failure to carry out the remedial plan will constitute a Material Breach for the purposes of Subsection 28.1(k) *(Service Provider Material Breach)*; and

(f) if the Province

(i) determines, in its reasonable opinion, that the breach of confidentiality obligations is material; or

(ii) does not Approve such remedial plan,

then such breach will constitute a Material Breach for purposes of Subsection 28.1(k) (*Service Provider Material Breach*).

12.7 Assigned Contracts.

For purposes of this Agreement, and in respect of those Subcontracts that are Assigned Contracts, the following provisions will apply:

(a) the Service Provider will enforce the existing provisions in such Assigned Contracts;

(b) the Service Provider will not, without the Province's Approval, reduce or eliminate existing provisions with respect to confidentiality, privacy and security;

(c) the Service Provider will use reasonable efforts to expand the confidentiality, privacy and security provisions of such Assigned Contracts to be in conformance with the requirements of this Agreement in respect thereof;

(d) the failure of an Assigned Contract to include provisions required by this Agreement to be included in a Subcontract, including the following, will not constitute a breach of this Agreement:

(i) provisions corresponding to the provisions of this Agreement that are required to be flowed down to Subcontractors,

(ii) any Privacy Obligations applicable to Subcontractors, including a requirement that External Personnel of the Subcontractor execute an External Personnel Agreement, or

(iii) in the case of an Assigned Contract that is a Material Subcontract, the provisions required to be included by Section 12.9 (*Additional Material Subcontract Terms*),

(e) when renewing or renegotiating such Assigned Contracts at the end of their respective current terms (and prior to any renewals or extensions thereof), the Service Provider will amend the terms to comply with the provisions of this Agreement; and

(f) as a condition of any renewal or renegotiation of any Assigned Contract at the expiry of its Term, or to any extension of an existing term of any Assigned Contract, and unless otherwise Approved by the Province (although any such Approval will not, and will not be deemed to, reduce any of the obligations of the Service Provider under the Privacy Obligations), the Service Provider will ensure that any such renewed, extended or renegotiated Assigned Contracts complies with the Privacy Obligations to the extent that the Privacy Obligations are applicable thereto, including the requirement that External Personnel of the Subcontractor accessing Personal Information execute an External Personnel Agreement.

Any breach of the confidentiality or the privacy and security provisions (if any) contained in the Assigned Contracts by Subcontractors will be deemed to constitute a breach of the confidentiality or the privacy and security provisions of this Agreement.

12.8 Material Subcontractors.

Any Subcontract entered into by the Service Provider for the performance of any part of the Services by a Subcontractor, where the Subcontractor meets the conditions or requirements set forth in **Schedule 20** *(Subcontractor Matters)* in respect thereof, will constitute a "**Material Subcontract**" to which the provisions of Section 12.9 (*Additional Material Subcontract Terms*), in addition to the provisions set forth in Section 12.3 (*General Contract Terms* (*Subcontractors*), will apply, but excluding therefrom any contracts that are Assigned Contracts.

12.9 Additional Material Subcontract Terms.

Unless consented to in writing by the Province, all Material Subcontracts entered into by the Service Provider will, in addition to the provisions set forth in Section 12.3 (*General Contract Terms* (*Subcontractors*), include the following provisions:

(a) provisions by which any Material Subcontractor who has or could have access to, use or disclosure of Personal Information in connection with the Services is bound to any applicable Privacy Obligations as identified in **Schedule 24** *(Privacy Obligations)*;

(b) provisions naming the Province as an intended third party beneficiary of the Material Subcontract and providing for the delivery by the Material Subcontractor of a certificate to such effect to the Province upon request;

(c) an agreement by both the Service Provider and the Material Subcontractor not to directly or indirectly assign the Material Subcontract to any Person without the Approval of the Province, not to be unreasonably withheld or delayed; and

(d) provisions entitling the Service Provider to terminate the Material Subcontract in response to a notice received from the Province under Section 12.13(a) (*Removal of Subcontractor*).

12.10 Extracts of Subcontracts.

During the Term of this Agreement, and at the request of the Province, the Service Provider will provide the Province with certificates signed by the Service Provider that have extracts of Material Subcontracts attached thereto, in a form sufficient for the Province to confirm the Service Provider's compliance with the obligations set forth in this Article 12 (*Subcontractors*). In connection therewith, the Service Provider will provide such certificate to the Province in respect of the Material Subcontracts described in the attached **Schedule 20** *(Subcontractor Matters)*, concurrently with the execution of this Agreement.

12.11 Consent to Use of Material Subcontractors.

The Service Provider will not use any Material Subcontractors in respect of the provision of any Services or other obligations performed under or in connection with this Agreement unless the Service Provider obtains the Approval of the Province, and for purposes hereof those Material Subcontractors described in **Schedule 20** *(Subcontractor Matters)* are hereby approved by the Province. Any request for Approval of a Material Subcontractor will include information regarding the components of the Services affected, the scope of the proposed Material Subcontract, the identity and qualifications of the proposed Material Subcontractor, whether the proposed Material Subcontractor is an Affiliate of the Service Provider, whether the proposed Material Subcontractor is a Canadian Entity, the foreign ownership (direct or indirect) of the proposed Material Subcontractor (if any), and the reasons for subcontracting the work in question.

12.12 Province Criteria for Material Subcontractors.

In considering a request for the Approval of a Material Subcontractor under the provisions of Section 12.11 (*Consent to Use of Material Subcontractors*), the Province will consider the reputation, financial stability, qualifications, applicable experience, ability, direct and indirect ownership, and availability of the Material Subcontractor, whether the Material Subcontractor who may have access to, or use or disclosure of Personal Information is a Canadian Entity, and the extent to which the Material Subcontractor could or would have access to, use or disclosure of any Personal Information, the purpose of such access, use and disclosure by (and by any External Personnel of) the Material Subcontractor. The Service Provider will not be required to provide to the Province any Subcontract (or draft Subcontract) with a Material Subcontractor (or proposed Material Subcontractor) in connection with a request for or to obtain the Province's Approval of the Material Subcontractor, except to the extent contemplated in Section 12.10 (*Extracts of Subcontracts*).

12.13 Removal of Subcontractor.

In the event that the Province determines, acting reasonably, that:

(a) the continued use of a Material Subcontractor will or could have a detrimental effect on the Province, and is therefore not in the best interests of the Province as a result of the Province having severed all other relationships with such Material Subcontractor due to the wilful misconduct, fraud or other forms of malfeasance by such Material Subcontractor; or

(b) the risk of a breach of the provisions of the *Freedom of Information and Protection of Privacy Act* is increased as a result of an Access Subcontractor ceasing to be a Canadian Entity or otherwise;

then the Province will give the Service Provider notice thereof (and specifying in detail the reasons therefor) through the Joint Executive Committee, requesting that such Material Subcontractor or Access Subcontractor be replaced. Promptly following receipt of such notice, the Service Provider will investigate the matters stated in the notice and discuss its findings with the Province through the Joint Executive Committee. If requested to do so by the Province (acting reasonably), the Service Provider will (within the timeframe specified by the Province after consultation with the Service Provider in respect of such timeframe) remove any access that the Material Subcontractor or Access Subcontractor may have to the Personal Information pending completion of the Service Provider's investigation and discussions with the Province. If, following such discussions with the Service Provider through the Joint Executive Committee, the Province reaffirms, acting reasonably, its request for the replacement of such Material Subcontractor or Access Subcontractor, then the Service Provider will, within ninety (90) days (or such different period of time as may be agreed to between the Parties through the Joint Executive Committee having regard to all of the surrounding circumstances) of such reaffirmation, replace such Material Subcontractor or Access Subcontractor with a new Material Subcontractor or Access Subcontractor of suitable qualifications, or will perform the applicable Services directly.

12.14 Other Business with Subcontractors.

Nothing contained in this Agreement will prohibit or otherwise restrict the Province from entering into agreements or other arrangements with any Subcontractor.

12.15 Suppliers.

The Service Provider may enter into contracts with Suppliers in respect of the Services (including for third party Software or for support or maintenance service) with such Suppliers as the Service Provider may select, provided that the Service Provider complies with any other applicable provisions of this Agreement regarding the use of Software in providing the Services. The following provisions will apply to contracts with Suppliers entered into by the Service Provider (other than contracts with Suppliers constituting Assigned Contracts) (it being understood that any Person who is given access to or use of Personal Information is a Access Subcontractor and not a Supplier for the purposes of this Agreement):

(a) all costs and expenses of such contracts with Suppliers will be the sole responsibility of the Service Provider, including any termination cost, penalties or other amounts payable in connection with such contracts;

(b) the Service Provider will ensure that the Suppliers have the required skill, qualifications and experience necessary to perform their obligations, and in the case of janitorial services, the Service Provider will retain bonded janitors only;

(c) the Service Provider will ensure that its Suppliers do not obtain access to Personal Information or Province Confidential Information by employing appropriate security policies, including, without limitation, a clean desk policy; and

(d) the Service Provider will not be relieved of any of its obligations in respect of the Services or under this Agreement as a result of any contracts with Suppliers, and the Service Provider will be responsible for all actions and failure to act of all of its Suppliers and the consequences thereof.

The Service Provider will monitor the performance of its Suppliers and will promptly address and remedy any performance issues or disputes in a manner which has no adverse impact on the nature, quality or delivery of the Services.

ARTICLE 13 – REPORTING AND ANNUAL OPERATING PLAN

13.1 Reporting Generally.

At all relevant times during the Term, the Service Provider will prepare or cause to be prepared, and will provide to the Province all reports and information required by the Province from time to time. The reporting requirements of the Province, which will be effective as and from the Hand-Over Date (and which excludes and reports or information to be provided by the Service Provider to the Province in connection with the Transition Services) is set forth in **Schedule 21** *(Reporting Requirements)*, and is subject to adjustment or amendment by the Parties through the Governance Process.

13.2 Annual Review of Reporting Requirements.

The Parties, through the Governance Process, will conduct an annual review of the then current reporting requirements under this Agreement and as set forth in **Schedule 21** *(Reporting Requirements)*, as the same may be adjusted or amended from time to time, and will consider any changes to the current reporting requirements as the Parties may determine to be appropriate or desirable.

13.3 Changes to Reporting Requirements.

The Parties acknowledge that the reporting requirements set forth in **Schedule 21** *(Reporting Requirements)* will evolve over the Term as a result of the addition of Services, changes made through the Change Order Process and otherwise. Subject to the provisions of **Schedule 21** *(Reporting Requirements)*, the Service Provider agrees that any changes to the reporting and information requirements of the Province, as contemplated under this Article 13 (*Reporting and Annual Operating Plan*), will not result in any increased Fees being payable by the Province. The Service Provider will at all times comply with the requirements of **Schedule 21** *(Reporting Requirements)*, as the same may be adjusted or amended from time to time, and will provide suggestions to the Province as to improvements, enhancements and changes to the reporting and informational requirements set forth in **Schedule 21** *(Reporting Requirements)*, for Approval by the Province through the Governance Process. Any changes that are made to the reporting requirements, as contemplated in this Section, will be deemed to be a Change Order for the purposes of this Agreement.

13.4 Format of Reports.

To the greatest extent possible, the Parties will use web-enabled reports and direct electronic access to data and query reports to meet the reporting and informational needs of the Province. The Parties agree to minimize the amounts and types of paper based reporting.

13.5 Annual Operating Plan.

The Service Provider will, with the co-operation and assistance of the Province through the Governance Process, prepare and provide to the Province an annual operating plan (the **"Annual Operating Plan"**) that will be the planning document utilized in the provision of the Services, consisting of:

(a) a summary of the financial and operational changes for the Services in the next most immediate Contract Year, based upon the most current annual estimate available;

(b) a survey, review and analysis of the Systems and resources used to provide the Services;

(c) strategies to assist in realizing the objectives set forth in Section 1.13 (*Objectives of the Parties*);

(d) an analysis of the operations by the Service Provider with recommendations for changes to reduce costs, improve efficiencies and improve the satisfaction of the customer's of the Services, the Province and Stakeholders;

(e) a description of any planned changes to the Services for the following Contract Year, to the extent known;

(f) a description of any proposed material changes in the way the Service Provider wishes to provide the Services;

(g) a review and analysis of any projects performed over the previous Contract Year and summary of recommended projects for the next immediate Contract Year, to the extent known;

(h) any planned System or resource acquisitions (including changes to the number and type of Personnel currently providing the Services, whether by an increase or decrease in the number and FTE of such Personnel) to provide for additional or decreased Service

capacity and volume, or to otherwise exploit new technological or business process developments;

(i) a description of the risk profile of the Service Provider, including a description of any material risks which could have an impact on the Service Provider's ability to provide the Services in accordance with Service Levels;

(j) a budget forecast setting out the estimated financial information in respect of the upcoming Contract Year, taking into account anticipated changes and information then available to the Service Provider (which budget will be consistent with the Economic Model, but subject to any changes having been made through the Change Order Process or otherwise); and

(k) such other matters as may be mutually agreed to by the Parties through the Governance Process.

13.6 Timing of Annual Operation Plan.

No later than 120 days prior to the commencement of the next Contract Year, the Service Provider will develop, prepare and provide to the Province, through the Governance Process, a proposed Annual Operating Plan for the next Contract Year, with the first Annual Operating Plan being delivered on or before **[insert date]**. Within 30 days following receipt of the proposed Annual Operating Plan, the Parties, through the Governance Process, will jointly Approve the Annual Operating Plan or discuss any modifications or changes required thereto, and the Service Provider will provide the Province, through the Governance Process, with a revised Annual Operating Plan incorporating such modifications or changes. Any Dispute with respect to the Approval of the Annual Operating Plan will be resolved through the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*).

13.7 Annual Confirmation.

The Service Provider will deliver a certificate to the Province, together with the Annual Operating Plan referred to in Section 13.5 (*Annual Operating Plan*), that contains a confirmation signed by a senior officer or director of the Service Provider stating that:

(a) a review of the activities of the Service Provider during the preceding Contract Year has been made under the supervision of such senior officer or director; and

(b) based upon the review referred to in paragraph (a) above, and to the best of the knowledge of such senior officer or director, after having made due inquiry, the Service Provider has fulfilled all of its obligations under this Agreement in all material respects (including, without limitation, the Privacy Obligations), and that no Material Breach (or any event which, with notice or lapse of time or both, could reasonably be determined to become a Material Breach) occurred during such Contract Year in respect of such obligations, and stating exceptions to any of the forgoing, if applicable.

ARTICLE 14 – MAINTENANCE OF RECORDS

14.1 Maintenance of Records.

During the Term and for a period of seven (7) years after the end of the Term (or such longer period as may be required by Applicable Law, or in the case of Subcontractors who cease to provide Services, seven (7) years after such Subcontractors have ceased to provide Services), the Service Provider will:

(a) maintain accurate and complete Records related to this Agreement and to the Services to be provided by the Service Provider under this Agreement (other than Records which have been returned to the Province by the Service Provider), as may be required or necessary in order for the following, provided that the Service Provider will not be required to retain any specific Record for a period of greater than seven (7) years except as required by Applicable Law:

(i) the Service Provider to meet any other reporting or record keeping requirements referred to in this Agreement, and

(ii) to enable the Province to verify compliance by the Service Provider with the terms of this Agreement and to ascertain the accuracy of all financial matters arising under this Agreement; and

(b) cause Subcontractors to maintain complete and accurate Records of the transactions and activities undertaken by such Subcontractors as part of the Services (other than Records which have been returned to the Province by the Service Provider), as may be required or necessary in order for the following, provided that the Subcontractor will not be required to retain any specific Record for a period of greater than seven (7) years except as required by Applicable Law:

(i) the Service Provider to meet any other reporting or record keeping requirements referred to in this Agreement, and

(ii) to enable the Province to verify compliance by the Subcontractor with the terms of this Agreement and to ascertain the accuracy of all financial matters arising under this Agreement.

Without limiting the generality of the foregoing, the Service Provider will ensure that all New Records with respect to the performance of the Services will conform with GAAP (to the extent applicable), the requirements of Applicable Laws, and the Province's Administrative Records Classification System (ARCS) and Operational Records Classification Systems (ORCS), as may be amended from time to time and notified by the Province to the Service Provider, subject to the Change Order Process.

14.2 Transferred Records.

The Province will arrange for the delivery of the Transferred Records to the Service Provider on or before the Hand-Over Date, in accordance with the records protocols described in the attached **Schedule 22** *(Records Protocols)*.

14.3 Custody of Province Records.

The Service Provider will have Custody of the Province Records from the later of the date that Custody is granted to the Service Provider by the Province or the date of the creation or coming into existence of the Province Records, in accordance with and subject to the provisions of this Agreement.

14.4 Control of Province Records.

The Province Records will remain the property and in the Control of the Province, and accordingly, they will continue to remain subject to the requirements of the British Columbia *Document Disposal Act, Electronic Transactions Act, Freedom of Information and Protection of Privacy Act* (British Columbia) and all Province Policies related, thereto, and the *Interpretation Act*. The Service Provider will comply

with the requirements thereof in respect of the Province Records as though each such Act or Policy applied to the Service Provider directly. In addition, the Service Provider will:

(a) not sell, transfer to the physical custody of another jurisdiction or Person, destroy or otherwise dispose of the Province Records without the Approval and direction of the Province, or as contemplated under this Agreement, and then, only in accordance with the protocols described in **Schedule 22** *(Records Protocols)*, and the provisions of Article 16 (*Privacy, Security and Confidentiality*);

(b) not under any circumstances, and without limiting the provisions of Article 16 (*Privacy, Security and Confidentiality*), use or disclose any Province Records except:

(i) on the prior written directions, or with the Approval, of the Province (which directions or Approval may be given by the Province at any time, in its sole discretion, or in response to a written request from the Service Provider specifying the particulars of the proposed use or disclosure of such Records), or

(ii) through the ordinary course provision of the Services as contemplated under the terms of this Agreement and in accordance with applicable Province Policies notified to the Service Provider from time to time;

(c) return the Province Records to the Province on the written instructions of the Province or as may otherwise be required or permitted in accordance with the provisions of this Agreement;

(d) at the request and expense of the Province, provide written or electronic copies of such Province Records for storage on the premises of the Province or of any applicable regulatory body or agency, as the Province may require;

(e) maintain the safe keeping and integrity of the Province Records in accordance with the records protocols set forth in the attached **Schedule 22** *(Records Protocols)* and with the provisions of Article 16 (*Privacy, Security and Confidentiality*);

(f) store all Province Records separately from other records of the Service Provider and identify them as Records of the Province; and

(g) provide the Province with copies of any Province Records, and permit the Province to have access to the Province Records with such access being in accordance with the provisions of Section 22.1 (*Access Rights*)).

The Province will comply with its obligations to the Service Provider in respect of the Province Records as set forth in **Schedule 22** *(Records Protocols).*

14.5 Final Return of Province Records.

Upon Termination of this Agreement, the Service Provider will deliver all such Province Records then in its Custody to the Province, including the performance of any obligations, steps or other requirements set forth in the Termination Assistance Plan. The Service Provider may, subject to the terms of Article 16 (*Privacy, Security and Confidentiality*), maintain sufficient copies of financial and other records following Termination of this Agreement, as it is required to maintain for tax and other statutory reasons in accordance with Applicable Laws.

14.6 Costs of Record Keeping.

The Service Provider acknowledges and agrees that all costs of record keeping contemplated in this Article 14 (*Maintenance of Records*) will be the responsibility of the Service Provider, and that compensation to the Service Provider in respect thereof is included in the Fees. For greater clarification, any Province Records delivered by the Service Provider to the Province at the request of the Province or pursuant to Sections 14.4 (*Control of Province Records*) and 14.5 (*Final Return of Province Records*), or **Schedule 22** *(Records Protocols)*, will thereafter be the responsibility (both financially and as to storage obligations) of the Province, unless such Province Records are returned to the Service Provider during the Term in accordance with the provisions of this Agreement.

14.7 Storage and Disposal of Records.

The Service Provider will transfer all Province Records identified by the Service Provider for storage, destruction or disposal to the Province in accordance with the record protocols more particularly described in **Schedule 22** *(Records Protocols)*, or as otherwise Approved by the Province. The Province will destroy any such Province Records if the Province determines it to be appropriate to do so. The Service Provider will not, without the Approval of the Province, dispose of or otherwise destroy any Province Records in its Custody at any time before the seventh (7^{th}) anniversary of the date that the final payment under this Agreement is made or of the date that all outstanding Disputes are settled, whichever is later.

14.8 Locations of Records.

Unless provided otherwise in this Agreement, and subject to the provisions of Section 5.1 *(Overview of Service Locations)*, the following provisions will apply in respect of all Province Records that contain any Personal Information:

(a) the Service Provider will maintain the Province Records in Canada at locations notified by the Service Provider to the Province in writing pursuant to Section 5.2 (*Service Locations*);

(b) the Service Provider will not relocate any such Province Records maintained pursuant to this Section without first notifying the Province in writing; and

(c) at no time will any Person have remote access to any Personal Information (including on any backup data) contained in the Province Records from any location outside of Canada, except as expressly Approved by the Province.

ARTICLE 15 – FEES AND PAYMENT TERMS

15.1 Fees.

In consideration of the performance of the Services, the Province will pay the Fees to the Service Provider, net of any amounts as contemplated pursuant to Article 8 *(Service Levels)*, or as otherwise contemplated in this Agreement. Except as otherwise expressly set forth in this Agreement, the Province will not be obligated to pay any other amounts to the Service Provider for the Service Provider's performance of the Services and its other obligations under this Agreement. Any expenses that the Service Provider incurs in the performance of the Services are included in the Fees, and accordingly, the Service Provider's expenses will not be separately reimbursable by the Province unless specifically provided otherwise under, or agreed pursuant to, the terms of this Agreement.

15.2 Invoices.

The Service Provider will provide the Province with monthly invoices, that conform to the payment requirements set forth in Section 15.3 (*Method of Payments*), for all Fees that are payable from time to time by the Province pursuant to this Agreement. Each invoice will be provided in hardcopy form, and if requested by the Province in electronic form compatible with the Province's financial computer systems, and in either case with the level of detail as may be requested by the Province from time to time to satisfy the Province's internal accounting requirements. The payment of any invoice by the Province will not be deemed to be Approval or acceptance of such invoice, and no such payment will preclude the Province from contesting any amount set forth in an invoice at any later date in accordance with the provisions of Section 15.6 (*Disputed Payments*).

15.3 Method of Payment.

The Province will pay the Fees to the Service Provider on the following terms:

(a) the Fees will be payable monthly, in arrears, prior to the date which is sixty (60) days after receipt by the Province of an invoice from the Service Provider in a form that is in compliance with this Agreement, such invoice not to be delivered by the Service Provider to the Province before the end of the Service period for which it relates;

(b) notwithstanding the payment date set forth above, interest on any overdue amounts will only be payable at the rates and in respect of the periods as set forth in the *Interest on Overdue Accounts Payable Regulation* (B.C. Reg. 215/83), as amended or replaced from time to time, and where such regulation has been revoked and not replaced, at the last rate and time period calculated thereunder; and

(c) all Fees calculated or otherwise set forth in this Agreement are inclusive of all applicable Taxes unless otherwise expressly stated in this Agreement (including, without limitation, the provisions of Section 15.4 (*Taxes*)).

15.4 Taxes.

The Services contracted for under this Agreement are for the Province, are being paid for with Crown funds, and are therefore not subject to GST. The Service Provider will collect, remit to the appropriate Taxing Authorities and report to the Province on all Taxes related to the Services to the extent that the same are included in the Fees, and to the extent that any of the Services attract PST, the Service Provider will add the same to the invoices for the Fees. The Service Provider will be responsible for and will arrange to pay all other Taxes relating to the Services including Taxes based on its own capital, net income, employment taxes of its own employees and for taxes on any property it owns.

15.5 Right of Set-Off.

Any amounts owed to the Province:

(a) by the Service Provider under this Agreement or otherwise in respect of the Services, including Service Level Credits, but excluding any amounts under Dispute;

(b) by the Service Provider under any other agreement entered into now or in the future between the Service Provider and the Province that is not related to this Agreement, but excluding amounts in dispute thereunder in accordance with its terms; and

(c) by the Service Provider's Affiliates pursuant to the Financial Guarantee;

may be set-off by the Province against Fees and other charges payable by the Province to the Service Provider under this Agreement, or may be deducted from any sum due or which at any time may become due to the Service Provider under this Agreement. To the extent that there are any amounts owing by the Service Provider to the Province upon the Termination of this Agreement, whether by credits or otherwise, and there are no further Fees to set-off such amounts, then the Service Provider will pay such amounts directly to the Province. The Province will give the Service Provider notice of such set-off under Section 15.5(b) above.

15.6 Disputed Payments.

Notwithstanding the payment of any Fees, the Province may dispute any amounts contained in an invoice within ninety (90) days of receipt of the invoice from the Service Provider. Notwithstanding the foregoing, if any overpayments by the Province should later be discovered as a result of an audit or investigation under Article 22 (*Audit Rights*) or otherwise, then the Province will be entitled to recover the amount of such overpayments by way of a Dispute, notwithstanding the fact that such overpayments are discovered after the expiry of such ninety (90) day period. In addition, the Province may withhold payment of a particular portion of Fees that the Province reasonably Disputes, subject to the following conditions:

(a) any amount so withheld will not exceed the amount alleged to be in error or not properly invoiced or payable, or for which no Services were performed;

(b) the Province provides to the Service Provider concurrently with the withholding of the disputed Fees, a detailed written explanation of the basis of the Dispute; and

(c) the Parties will promptly settle the Dispute regarding such amount in accordance with the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*).

Any interest accrued on any amount owed to or overpaid by the Province will be apportioned in the same manner as in the resolution of such disputed Fees. Any payment disputes will not affect the Service Provider's obligation to provide the Services under this Agreement at the agreed Service Levels or in accordance with any other of the Service Provider's obligations under this Agreement.

ARTICLE 16 – PRIVACY, SECURITY AND CONFIDENTIALITY

16.1 Privacy Obligations.

The Service Provider will at all times, and will ensure that its Personnel, and to the extent applicable in accordance with the provisions of **Schedule 24** *(Privacy Obligations)* its Subcontractors and External Personnel, comply with the obligations and requirements set forth in **Schedule 24** *(Privacy Obligations)*, as such are amended from time to time in accordance with this Agreement (the "**Privacy Obligations**").

16.2 Foreign Disclosures.

The Service Provider expressly acknowledges and agrees that it is subject to the laws of British Columbia and the laws of Canada applicable in British Columbia with respect to this Agreement and the performance of the Service Provider's obligations under this Agreement, and it is not subject to any Foreign Disclosure Laws including, without limitation, any orders, directives, rulings, requirements, judgments, injunctions, awards or decrees, decisions, or other requirements issued pursuant to any Foreign Disclosure Laws, or any directions or requests from any Affiliate of the Service Provider in

respect of the same, and in each case, related to any Personal Information (each a "**Disclosure Order**"). The Service Provider will immediately inform the Province if the Service Provider receives a Disclosure Order. Upon receipt of a Disclosure Order, the Service Provider will not disclose any Personal Information in response thereto and the Service Provider will at all times act in accordance with the terms and conditions of this Agreement including, without limitation, the Privacy Obligations. Any breach of this Section will be a Material Breach under this Agreement. The provisions of this Section represent a lawful restriction on the Service Provider, being a Person governed by the laws of British Columbia and the laws of Canada applicable in British Columbia. The Service Provider will flow through the requirements of this Section to any Access Subcontractors, to apply to the Access Subcontractors, *mutatis mutandis*.

16.3 Corporate Structure and Corporate Chart.

As of the date of this Agreement, and as at the Hand-Over Date, the corporate organizational chart, indicating all shareholdings to the ultimate indirect shareholder (other than the shareholdings of a public company listed on a recognized stock exchange) of the Service Provider, the Performance Guarantor and the Financial Guarantor each a ("**Corporate Structure**"), are as set forth in **Schedule 25** *(Corporate Chart)*. Throughout the Term, the Service Provider will provide the Province with an updated Corporate Structure from time to time forthwith upon any changes being made thereto; provided that the requirements of this provision will in no way provide the Service Provider with any relief from, or be deemed to be a waiver of, the provisions of Section 31.2 (*Assignment by Service Provider*). Unless agreed otherwise by the Province, for so long as the Service Provider or the Performance Guarantor has, or could have, disclosure or use of, or access to any Personal Information in connection with the performance of the Services under this Agreement, or in connection with the application of the Performance Guarantee, as the case may be, the Service Provider and the Performance Guarantor will be and remain under the direct Corporate Control of a Canadian Entity, and any failure of the Service Provider or the Performance Guarantor to remain so controlled will be deemed to be a Material Breach under Section 28.1 (*Service Provider Material Breach*), and will give rise to the right of the Province to terminate this Agreement pursuant to Section 28.2 (*Remedies of the Province*).

16.4 Canadian Entities.

Throughout the Term, the Service Provider will ensure that the Access Subcontractors who are not individuals are corporations, partnerships, limited partnerships, or other similar entities that are incorporated or created under the laws of Canada or under the laws of any province of Canada (each a "**Canadian Entity**"), and that the Access Subcontractors who are individuals are not Foreign Employed Individuals. Unless agreed otherwise by the Province, and for so long as any Access Subcontractor has or could have any access to, or use or disclosure of, any Personal Information in connection with the performance of the Services under this Agreement, the Service Provider will ensure that:

(a) in the case of Access Subcontractors who are individuals, the Access Subcontractor are not, and do not become, a Foreign Employed Individual; and

(b) in all other cases, the Access Subcontractors are and remain a Canadian Entity, and unless otherwise Approved by the Province, a Canadian Entity that is Corporately Controlled by a Canadian Entity or by individuals who are not Foreign Employed Individuals.

16.5 Acknowledgement.

The Service Provider acknowledges that in the performance of the Services, the Service Provider will be given access to and Custody of highly confidential and sensitive information, including Province

Confidential Information, and that the confidentiality, privacy and security of such information, and in particular the Personal Information, is of paramount importance to the Province.

16.6 Safeguarding Confidential Information.

Each of the Parties acknowledges and agrees that all Confidential Information of the other Party, whether received or created before or after the Hand-Over Date, will be received in the strictest confidence and will be held and used only in accordance with and subject to the terms of this Agreement. A Party receiving the Confidential Information of the other Party will retain such information in confidence and will treat such information in accordance with the terms of this Agreement (including the Privacy Obligations), and with a degree of care no less than the degree of care that the receiving Party employs for the protection of its own Confidential Information of a similar nature; provided that in any event the Service Provider will use a degree of care to protect such Confidential Information that is appropriate to the nature of the information and is in accordance with prudent industry practice for the ***[insert industry]*** in Canada. Without limiting the generality of the foregoing, and subject to the Change Order Process, the Service Provider further agrees to comply with such confidentiality, privacy and security Directives as issued by the Province from time to time.

16.7 Permitted Disclosure and Use of Confidential Information.

Subject to the Privacy Obligations and Section 16.2 (*Foreign Disclosures*), a Party may use or disclose relevant aspects of the other Party's Confidential Information:

(a) only to the extent necessary to perform its obligations and exercise its rights under this Agreement;

(b) only to its Personnel, Subcontractors and External Personnel (and in the case of the Province, its employees, contractors, professional advisors and agents) to the extent that such disclosure and use thereof is necessary for the performance of the receiving Party's rights or obligations under this Agreement, and provided that such Persons have an actual need to know such information and have signed non-disclosure agreements as required by this Agreement (to the extent applicable), it being agreed between the Parties that the provisions of this paragraph will in no way restrict or otherwise limit either Party from disclosing the Confidential Information of the other Party, to the extent necessary, to the receiving Party's legal advisors in the course of obtaining legal advice in connection with this Agreement, provided that the solicitor client privilege with respect thereto is not waived by the receiving Party in respect of such disclosure; and

(c) in the case of a disclosure of the Service Provider's Confidential Information by the Province, for purposes of undertaking any procurement or related process in connection with the selection of an Alternative Service Provider, provided that:

  (i) such disclosure does not include any of the Service Provider's costing or other internal financial information,

  (ii) any third parties to whom such disclosure is made first execute and deliver to the Province a Non-Disclosure Agreement and the Province provides such executed Non-Disclosure Agreement to the Service Provider, and

  (iii) such disclosure will be restricted to the Service Provider Confidential Information necessary to enable such parties to participate in such procurement or related process.

16.8 Province Permitted Disclosure.

Notwithstanding the provisions of this Article 16 (*Privacy, Security and Confidentiality*), the Province may disclose the Service Provider Confidential Information as may be required by the provisions of any Applicable Laws, including the *Freedom of Information and Protection of Privacy Act* (British Columbia), as contemplated in Section 16.10 (*Disclosure Compelled by Law*) and as required by the Province in order to prevent any actual or reasonably anticipated disclosure of Personal Information. For purposes thereof, the Service Provider acknowledges that the Non-Disclosure Agreements referred to in Section 16.7 (*Permitted Disclosure and Use of Confidential Information*) will be subject to the requirements and obligations of that Act.

16.9 Exceptions to Obligation of Confidentiality.

Subject to the Privacy Obligations and Section 16.2 (*Foreign Disclosures*), the obligations of confidentiality contained in this Article 16 (*Privacy, Security and Confidentiality*) will not apply to any Confidential Information of the other Party to the extent that the receiving Party can reasonably demonstrate that such Confidential Information:

(a) was, at the time of disclosure to the receiving Party, in the public domain;

(b) after disclosure to the receiving Party, is published or otherwise becomes part of the public domain through no fault of the receiving Party, and where the receiving Party is the Service Provider, through no fault of the Service Provider's Affiliates or Subcontractors;

(c) was in the possession of the receiving Party at the time of disclosure to the receiving Party, and was not the subject of a pre-existing confidentiality obligation;

(d) was disclosed independently to the receiving Party by a third party who, insofar as the receiving Party was aware, was not subject to any confidentiality obligations in respect thereof, and in any event, provided that such information was not of a nature that had it been the Confidential Information of the receiving Party, the receiving Party would have required that it be kept confidential;

(e) was independently developed by the receiving Party without the use of any Confidential Information of the other Party;

(f) is disclosed with the prior Approval of the other Party, but only to the extent Approved by the other Party;

(g) is Service Provider Confidential Information and such information is required to be disclosed by the Province under the *Freedom of Information and Protection of Privacy Act* (British Columbia); or

(h) is Service Provider Confidential Information and such information is required to be disclosed by the Province in order to comply with Province Policies.

16.10 Disclosure Compelled by Law.

Subject to the Privacy Obligations and Section 16.2 (*Foreign Disclosures*), a Party will not be considered to have breached its confidentiality obligations under this Article 16 (*Privacy, Security and Confidentiality*) for disclosing any Confidential Information of the other Party to the extent that such

disclosure is required to satisfy any Applicable Laws and, subject to Section 16.11 (*Disclosure of Personal Information*), expressly excludes Personal Information, provided that the Party required to make such disclosure (the "**Compelled Party**"):

(a) promptly upon receiving any such request and within a reasonable time prior to disclosure (if possible), notifies the other Party of the terms and circumstances of the requested disclosure;

(b) consults with the other Party regarding the nature and scope of such request and the response or other position that the Compelled Party intends to take with respect to such request;

(c) does not obstruct or interfere with, and to the extent practical, permits the other Party to obtain, a protective order or other remedy to prevent, object to, enjoin, narrow the scope of, or otherwise contest the requested disclosure;

(d) if the other Party is unable to obtain a protective order or other similar remedy within a time period that is appropriate in the circumstances, then the Compelled Party will only disclose such of the Confidential Information that it is legally obligated to disclose; and

(e) makes and reasonably pursues a request, that is reasonable and customary in the circumstances, to the applicable Governmental Authority, for confidential treatment of the information to be disclosed pursuant to such Applicable Laws.

16.11 Disclosure of Personal Information.

In respect of the Personal Information that constitutes Province Confidential Information, the Service Provider will not disclose to any Person or allow any Person to access or use, and will ensure that none of the Personnel, Subcontractors, or External Personnel disclose to any Person or allow any Person to access or use, the Personal Information, except:

(a) if, and in the manner expressly permitted pursuant to, the Privacy Obligations or to the provisions of the *Freedom of Information and Protection of Privacy Act* (British Columbia);

(b) as expressly Approved by the Province; or

(c) pursuant to an order of a Canadian court of competent jurisdiction in accordance with Section 16.12 (*Court Order Disclosure*).

16.12 Court Order Disclosure.

If the Service Provider is required, in order to satisfy any Applicable Laws, to disclose to any Person or to allow any Person to have access to any Personal Information other than as permitted in Subsections 16.11(a) to (b) (*Disclosure of Personal Information*), then the Service Provider will not disclose or allow access to the same unless and until the Service Provider:

(a) has provided the Province with written notice of such requirement;

(b) the Service Provider and the Province (at the Province's option) have appeared before a Canadian court having competent jurisdiction; and

(c) such Canadian court has ordered that the Service Provider disclose or allow access to the Personal Information.

16.13 Notification of Unauthorized Use of Confidential Information.

Each Party will:

(a) promptly notify the other Party of any unauthorized possession, use, access or disclosure, or attempt to effect the same, of the other Party's Confidential Information by any Person that has become known to such Party;

(b) promptly furnish the other Party with details of such unauthorized possession, use, access or disclosure, or attempt to effect the same, and assist the other Party in investigating or preventing the recurrence of any unauthorized possession, use, access or disclosure, or attempt to effect the same, of the other Party's Confidential Information;

(c) cooperate with the other Party in any litigation and investigation against third parties deemed necessary by the other Party to protect its Confidential Information, to the extent such litigation or investigation is related to this Agreement; and

(d) promptly use best efforts to prevent a recurrence of any such unauthorized possession, use, access or disclosure of the other Party's Confidential Information.

The Service Provider will reimburse any direct expenses incurred by the Province as a result of compliance by the Province with this Section.

16.14 Breach of Confidentiality.

In the event of a breach of this Article 16 (*Privacy, Security and Confidentiality*), and to the extent available pursuant to Applicable Laws (including, without limitation, the *Crown Proceeding Act* (British Columbia)), the non-defaulting Party will be entitled to preliminary and permanent injunctive relief, as well as an equitable accounting of all profits and benefits arising out of such breach, which remedy will be in addition to any other rights or remedies to which the Party may be entitled under this Agreement or otherwise under any Applicable Laws.

16.15 No Rights to Confidential Information.

Nothing contained in this Article 16 (*Privacy, Security and Confidentiality*) will be construed as obligating a Party to disclose its Confidential Information to the other Party, or is granting or conferring on a Party, expressly or implied, any right, title or interest or any licence in or to the Confidential Information of the other Party.

16.16 Ownership of Province Confidential Information.

The Province Confidential Information is and will remain the property of the Province. Subject to applicable security procedures and System availability, the Province will have complete and unrestricted Control and access at all times of and to the Province Confidential Information and, as part of the Services, the Service Provider will provide access thereto as may be requested by the Province from time to time, including such access as will enable the Province to make complete copies of all Province Confidential Information. Control of the Province Confidential Information is vested solely in the Province and nothing in this Agreement will in any way be construed to grant Control of the Province Confidential Information to the Service Provider or any other Person. The Service Provider will at all

times adhere to the directions of the Province with respect to Province Confidential Information. On the Province's request, at any time during the Term or upon any Termination, the Service Provider will promptly return to the Province, in the format and on the media requested by the Province, all or any part of the Province Confidential Information, and erase or destroy all or any part of the Province Confidential Information in the Service Provider's or in any Service Provider Group member's possession, or in each case to the extent so requested by the Province.

ARTICLE 17 – BUSINESS CONTINUITY

17.1 General.

As part of the Services, the Service Provider will:

(a) on or before the Hand-Over Date, and as part of the Transition Services, review the Province's existing Business Continuity Plan for the Services and update such plan as may be reasonably determined necessary by the Service Provider, and Approved by the Province;

(b) ensure that the Business Continuity Plan at all times expressly address all Force Majeure Events and Labour Disruptions;

(c) from and after the Hand-Over Date, assume all responsibility for the establishment and maintenance (including all related management, training, planning, plans, work products and deliverables) of the Business Continuity Plan for the Services, having regard to the roles and responsibilities of the Parties as set forth in Section 17.2 (*Roles and Responsibilities*);

(d) be responsible for all costs in respect of any updates to the Business Continuity Plan, unless specifically agreed otherwise by the Parties under the terms of this Agreement.

For greater clarification, the updated Business Continuity Plan Approved by the Province as contemplated in paragraph (a) above will be implemented and maintained by the Service Provider for the Term of this Agreement, subject to further amendments by the Service Provider in accordance with the terms of this Article 17 (*Business Continuity*), and will thereafter be, and be deemed to be, the Business Continuity Plan for purposes of this Agreement.

17.2 Roles and Responsibilities.

The roles and responsibilities of the Parties in respect of the Business Continuity Plan and the Disaster Recovery Plan for the Services will be as set forth in this Article 17 (*Business Continuity and Disaster Recovery*) including, without limitation, the following:

(a) the roles and responsibilities of the Province are as follows:

(i) to lead the Ministry's business continuity planning,

(ii) to provide standards and templates to the Service Provider if and to the extent that the Province requires that the Service Provider use or follow the same,

(iii) at the request of the Service Provider, to provide clarification regarding the interpretation or application of applicable Province Policy,

(iv) at the option of the Province, to participate in and review any test activities of the Business Continuity Plan for the Services,

(v) to review the Business Continuity Plan for the Services from time to time to ensure that they comply with and otherwise conforms to applicable Province Policy (including any applicable Ministry policy) and the requirements of this Agreement, and to the extent that the Province determines, in its sole discretion, that the Business Continuity Plan does not so comply, then upon receipt of written notice thereof from the Province the Service Provider will forthwith update and amend the Business Continuity Plan to the extent required for the Business Continuity Plan to be fully compliant with the applicable Province Policy (including any applicable Ministry policy) and the requirements of this Agreement,

(vi) to communicate with Stakeholders regarding the integration and co-ordination of the Service Provider's Business Continuity Plan for the Services with those of the Stakeholders, and

(vii) to establish applicable Recovery Time Objectives in respect of the Business Continuity Plan for the Services, in consultation with the Service Provider through the Governance Process; and

(b) the roles and responsibilities of the Service Provider are as follows:

(i) to comply with applicable Province Policy (and any applicable Ministry policy), and the terms of this Agreement, relating to business continuity and disaster recovery, and upon receipt of a written notice from the Province that the Business Continuity Plan does not so comply with the same, to forthwith update and amend the Business Continuity Plan to the extent required for the Business Continuity Plan to be fully compliant with the applicable Province Policy (including any applicable Ministry policy) and the requirements of this Agreement,

(ii) to provide business continuity and disaster recovery services to the Province and to take responsibility for the Business Continuity Plan in respect of the Services, in accordance with the provisions of this Article 17 (*Business Continuity*),

(iii) to ensure that its Subcontractors are able to meet the requirements of the Business Continuity Plan for the Services to the extent applicable to them,

(iv) to provide the Province with information and cooperation (and participation) in respect of the Business Continuity Plan for the Services as may be requested by the Province from time to time,

(v) to notify the Province (through the **[insert office e.g., AMO]**) in the event of the declaration of a Disaster and the resulting requirement to activate a Business Continuity Plan for the Services, and

(vi) to ensure the effectiveness, preparedness and ability of the Service Provider to execute the Business Continuity Plan for the Services.

17.3 Service Provider Representative.

The Service Provider will designate a "Business Continuity Representative", who may be identified as a Key Position, to be responsible for:

(a) the upkeep, testing and implementation of the Business Continuity Plan for the Services; and

(b) acting as the liaison with the Province to ensure the integration of the Service Provider's Business Continuity Plan for the Services with those of the Province and Stakeholders (to the extent applicable).

The Service Provider will also designate an alternate representative (or representatives), who need not be a Key Position, to act as the "Business Continuity Representative" if the original designated representative is unavailable for any reason.

17.4 Plan Management and Annual Reviews.

From and after the Hand-Over Date, the Service Provider will be responsible for managing the continuity of the Services, in accordance with the business continuity and disaster recovery Province Policies, and pursuant to the Business Continuity Plan for the Services. The management of the Business Continuity Plan will include, without limitation, the following:

(a) the performance in each Contract Year of business impact assessments in respect of the Services;

(b) the performance in each Contract Year of strategic risk assessments in respect of the Services;

(c) the development of risk mitigation and business continuity and disaster recovery treatments in respect of the Services;

(d) to the extent applicable, the development of a Business Continuity Plan specifically for any essential Services as may be so notified by the Province to the Service Provider from time to time; and

(e) a review and update of the Business Continuity Plan for the Services at least once per Contract Year.

Any changes to the Business Continuity Plan for the Services may be submitted by either Party to the other in accordance with the Governance Process, or through the Change Order Process, as applicable. For greater clarification, the Province will have the right to review any changes to the Business Continuity Plan for the Services to ensure compliance with Province Policy (and any applicable Ministry policy), and the terms of this Agreement, prior to implementation thereof.

17.5 Recovery Time Objectives.

The Recovery Time Objectives for the Services will be reviewed, confirmed and Approved by the Parties through the Governance Process within **[insert number]** after the Hand-Over Date. Thereafter, and in each Contract Year, the Parties will review the Recovery Time Objectives, and will mutually agree on any revisions to the Recovery Time Objectives through the Governance Process, or will otherwise amend the Recovery Time Objectives through the Change Order Process, as applicable.

17.6 Testing of Business Continuity Plan.

The testing of the Business Continuity Plan for the Services will be performed by the Service Provider in accordance with applicable Province Policy in respect thereof. The testing will consist of process walkthrough and awareness testing (as opposed to full production testing), except as specifically provided otherwise below. Such testing will include the following (to the extent consistent with the foregoing and as may applicable to the Service Provider):

(a) the Service Provider will complete a test of the Business Continuity Plan for the Services within such period following the Hand-Over Date as is specified in **Schedule 5** (*Special Terms*);

(b) the Service Provider will test the Business Continuity Plan for the Services with such frequency following the initial test described in paragraph (a) above as is specified in **Schedule 5** (*Special Terms*);

(c) the testing will include fail-over testing from the Service Provider's production facility to its back-up site;

(d) the Service Provider may carry out the fail-over tests at such times and in such manner (including a single complete test or successive partial tests) as the Service Provider deems appropriate;

(e) the Service Provider will conduct the testing in a manner that causes minimal disruption to the ongoing operations of the Services, and in full consultation with the Province;

(f) the Service Provider will complete a test of the Business Continuity Plan for the Services within such period as is specified in **Schedule 5** (*Special Terms*) of implementing any material change in respect of the Services (including, without limitation, any material change in the technology, processes, facilities, infrastructure, Systems or Recovery Time Objectives), for purposes of determining the impact of such material changes to the Services and the effectiveness of the Business Continuity Plan in respect thereof;

(g) the Province will have the right to participate in any testing of the Business Continuity Plan for the Services as an observer in the testing process and to review any results of such testing;

(h) within thirty (30) days of any testing conducted by the Service Provider in respect of the Business Continuity Plan for the Services, the Service Provider will prepare and submit to the Province, through the Governance Process, a report detailing the results of such testing and listing any deficiencies in respect thereof, together with the Service Provider's proposed action plan and assigned responsibilities and timelines that will be undertaken by the Service Provider to address such deficiencies, and the Service provide will forthwith take all such steps and to all such things as may be necessary to carry-out and implement such action plan.

17.7 Actual Disaster.

In the event of a Disaster, or either Party's anticipation of a Disaster, the following provisions will apply:

(a) if the Service Provider is prevented from, or delayed in, performing any of its obligations under this Agreement as a result of the Disaster, or anticipates that it will be so prevented

or delayed, then the Service Provider will promptly notify the Province thereof, and will provide the Province with a follow-up written notice within two (2) Business Days of the Service Provider becoming aware of the potential disruption, non-performance or delay, the particulars thereof including details of the nature of the event causing the same, its expected duration and the obligations under this Agreement that will be affected as a result;

(b) the Service Provider will continue to provide detailed reports to the Province with respect to such disruption, non-performance or delay, on a timely basis during the continuance thereof;

(c) the Service Provider will restore all Services in accordance with the Business Continuity Plan for the Services (including the redeployment or reassignment of other available personnel to assist with the implementation of the Business Continuity Plan), having regard to the nature and extent of the Disaster and its impact on the Services, the Province, the Stakeholders and other customers of the Services;

(d) to the extent that the Disaster is not addressed or not fully addressed in the Business Continuity Plan for the Services, the Service Provider will use its best efforts to restore the Services;

(e) within thirty (30) days of the recovery of the Services as a result of the implementation of the Business Continuity Plan for the Services, the Service Provider will provide the Province with a written report detailing the root cause of the disruption, the steps taken by the Service Provider in respect thereof, and any recommendations that the Service Provider may have with respect to improving the Business Continuity Plan for the Services (including the responsibilities and timelines referred to therein);

(f) subject to the provisions of Article 30 (*Force Majeure and Labour Disruption*), if contrary to the Recovery Time Objectives, or as a result of the negligence of the Service Provider, the Service Provider does not materially restore the Services in accordance with the Business Continuity Plan for the Services, then the Province will be entitled to procure such services from another service provider (to the extent possible), and may off-set the costs thereof against the Fees payable to the Service Provider;

(g) notwithstanding the foregoing, the Province will retain the right to audit, sign-off and confirm the full recovery of the delivery of the Services following the implementation of the Business Continuity Plan for the Services; and

(h) there will be no Service Level Credits assessed or otherwise applied by the Province against the Service Provider during the continuance of the Disaster and until full recovery of the delivery of the Services pursuant to the Business Continuity Plan, provided that the Service Provider complies, in all material respects, with its obligations under the provisions of this Article 17 (*Business Continuity*).

ARTICLE 18 – TECHNOLOGY, ARCHITECTURE AND IMPROVEMENTS

18.1 Architecture Standards.

In addition to the obligations otherwise set forth in this Agreement, the Service Provider will implement the Province's existing technical architecture standards and guidelines to the same extent as such standards and guidelines are themselves complied with by the Province as of the Hand-Over

Date, as such standards are updated or revised by the Province from time to time (subject to the Change Order Process). The Service Provider will advise the Province of any significant incompatibilities known to the Service Provider that would result from changes to such standards. If the Province requests the Service Provider's assistance to document technical architecture standards, then the Service Provider will deliver a draft manual setting out the technical architecture standards within **[insert number]** months of the request. The Service Provider will update the Manual from time to time during the term as such standards change (and in accordance with the Change Order Process). The architectural standards and guidelines will form part of the Manual.

18.2 Technology Improvements and Currency.

The Service Provider will provide the Services by maintaining the supporting technologies at an appropriate level of currency and in a manner that will support the Parties' efforts to achieve the objectives set forth in Section 1.13 (*Objectives of the Parties*), and to comply with the Service Levels and the Privacy Obligations. Except as specifically, provided otherwise in this Agreement, the Service Provider will determine the appropriate levels of technology currency, and throughout the Term will identify and implement technology improvements, all with the Approval of the Province, and in accordance with the applicable provisions of **Schedule 5** (*Special Terms*). Except where the Province agrees in writing that such implementations are not necessary, the Service Provider will report to the Province at the end of each quarter throughout the Term, demonstrating its actions taken to meet its obligations relating to improvements in technology set forth in this Section 18.2 (*Technology Improvements and Currency*). In addition, the Service Provider will report to the Province at the end of each **[insert period, quarter, Contract Year, etc.]** throughout the Term, setting forth the actions or steps that the Service Provider has taken to meet its obligations relating to improvements in technology as set forth in this Section.

18.3 Material Technology Change.

Before making any material changes to the suppliers of technology to be used by the Service Provider in performing the Services, the Service Provider will consult with the Province in respect thereof through the Governance Process, and will obtain the Approval of the Province to any such change, unless the requirement to obtain such Approval is waived in writing by the Province on a case by case basis.

18.4 Technology Presentations.

At the Province's request and cost, the Service Provider will facilitate the attendance of the Province personnel at any presentation offered to the Service Provider by any technology vendor whose software, equipment or materials are used, or are being considered by the Service Provider for use, directly or indirectly in a material manner in the provision of Services, except in the event that the Service Provider cannot obtain the consent of such technology vendor.

18.5 System Contaminants.

The Service Provider will ensure that all Systems provided or used by it, or by its Subcontractors or Suppliers, to provide the Services do not and will not contain any virus, Trojan horse, worm, backdoor, shutdown mechanism or similar software, code or program which is intended to, is likely to or has the effect of disabling, denying authorized access to, damaging or destroying, corrupting or affecting the provision of the Services or the normal use of any of the Service Provider's or the Province's Systems, networks or software, or any data on or used in conjunction therewith (each a **"Contaminant"**). The Service Provider will not insert, or knowingly permit any third party to insert, a Contaminant into any of the Systems used to provide the Services. In the event the Service Provider becomes aware of the

existence of a Contaminant, it will notify the Province thereof and will remove the Contaminant in a prompt and co-ordinated manner so as to minimise the spread and impact of such Contaminant.

18.6 System Protection Features.

To the extent that any Software developed or created by the Service Provider for use in connection with the Services, or accessed by or delivered to the Province by the Service Provider, contains protection features designed to prevent copying or the use of such Software or other unauthorized access, to disable or erase Software or data, to shut down all or any portion of the Services or to perform other like actions, the Service Provider will provide the Province with the necessary key, password or other means such that the Province will have continued access and use of such Software without technical limits of any kind.

ARTICLE 19 – INTELLECTUAL PROPERTY AND PROPRIETARY RIGHTS

[NOTE – these provisions will require amendment depending upon the use of third party software under existing corporate licenses of either party.]

19.1 Ownership of Other Assets.

Except as expressly provided in this Agreement, the Province will be and remain the exclusive owner of all rights, title and interest in and to all assets and property provided by the Province to the Service Provider, including any assets to which the Service Provider is given access to by the Province from time to time during the Term.

19.2 Ownership of Province Software and Modifications.

The Province will be and remain the sole and exclusive owner of all right, title and interest, including all Intellectual Property Rights, in and to:

(a) all Province Proprietary Software;

(b) all Modifications of the Province Proprietary Software, whether made by or on behalf of the Province or the Service Provider, separately, jointly or with any other Person (including any of the Service Provider, Subcontractors, Personnel or External Personnel), and including where any Province Proprietary Software or any Modifications thereto has been incorporated into any the Service Provider Software; and

(c) all Modifications to the Service Provider Software that are used in connection with the Services provided under this Agreement, whether made by or on behalf of the Service Provider (or its Subcontractors or its or their Affiliates, as the case may be) or the Province, separately or jointly or with any other Person, and including where any Modifications have been incorporated into any of the Service Provider Software, but subject in all cases to the provisions of Section 19.7 (*Service Provider License to Modifications*).

Except as expressly provided otherwise under this Agreement, nothing in this Agreement or in the relationship between the Parties will confer any right or license in or upon the Service Provider in respect of the Province Confidential Information.

19.3 Assignment by the Service Provider.

If, notwithstanding Section 19.2 (*Ownership of Province Software and Modifications*), the Service Provider retains, acquires or owns any right, title or interest, including any Intellectual Property Rights, in or to any Province Proprietary Software or any Modifications thereto, then the following provisions will apply:

(a) the Service Provider will assign, and for no further consideration and without any further act or formality does hereby irrevocably assign, to the Province all of the Service Provider's worldwide right, title and interest in and to any Province Proprietary Software and any Modifications thereto, including all Intellectual Property Rights therein, free and clear of all Liens, but subject to the provisions of Section 19.5 (*Use of Province Software for the Services*);

(b) if and to the extent that the assignment pursuant to this Section is not effective on the date hereof or on any future date, either generally or pursuant to any Applicable Laws, then any and all right, title and interest, including the Intellectual Property Rights, in and to any Province Proprietary Software or Modifications thereto that is retained, acquired or owned by the Service Provider (collectively, the "**Province Trust Rights**"), will be held by the Service Provider in trust for the exclusive benefit and use of the Province and its designates, except for the rights granted to the Service Provider pursuant to Section 19.5 (*Use of Province Software for the Services*) and Section 19.7 (*Service Provider License to Modifications*); and

(c) the Service Provider will execute and deliver to the Province such reasonable transfers, assignments, documents and instruments (promptly upon receipt thereof from the Province) as may be necessary to transfer and assign to the Province the Province Trust Rights, free and clear of all Liens, and will otherwise cooperate with the Province to give effect to, record and register the Province's ownership of the Province Trust Rights.

19.4 Personnel, Subcontractors and External Personnel.

The Service Provider will ensure that all Personnel, Subcontractors and External Personnel will:

(a) by duly executed written agreement or by operation of law, irrevocably and unconditionally sell, assign and transfer to the Service Provider all right, title and interest, including all Intellectual Property Rights, that they may have in or to any or all Province Proprietary Software and all Modifications thereto, such that the assignment by the Service Provider pursuant to Section 19.3 (*Assignment by the Service Provider*) includes any such right, title and interest, including all Intellectual Property Rights, of the Personnel, Subcontractors and External Personnel; and

(b) by duly executed written agreement or waiver document, irrevocably waive all non-transferable rights, including moral rights, that they have or may have in any Province Proprietary Software or any Modifications thereto, in favour of the Service Provider, the Province and their respective successors and assigns.

If requested by the Province, and without limiting the Service Provider's obligations pursuant to this Section, the Service Provider will itself execute, and will obtain the execution by all Personnel, Subcontractors and External Personnel of all reasonable formal assignment documents requested and prepared by the Province, and the execution of all lawful oaths and applications for registration of the same in Canada and in foreign countries.

19.5 Use of Province Software for the Services.

Subject to the provisions of this Agreement, the Service Provider will have the non-exclusive right during the Term, without cost or charge but subject to any third party rights as notified by the Province to the Service Provider, to use and copy the Province Proprietary Software and create and use any Modifications thereto, for the purpose of providing the Services pursuant to, and in accordance with, the terms of this Agreement, but subject to any restrictions, license terms or polices as reasonably determined by the Province, and any third party rights therein, all as may be notified in writing by the Province to the Service Provider. In connection therewith, the following provisions will apply:

(a) the Province will provide the Service Provider with any necessary third party rights to give effect to the foregoing rights granted to the Service Provider;

(b) the foregoing rights granted to the Service Provider do not give the Service Provider the right, and the Service Provider is not authorized, to market the Province Proprietary Software or Modifications thereto or to authorize any other Person to use the Province Proprietary Software or Modifications thereto (other than the Service Provider's Subcontractors who require the same for purposes of, and in connection with, the delivery of the Services to the Province);

(c) the Province may authorize or licence any third parties to use the Province Proprietary Software and any Modifications thereto during the Term, it being acknowledged that to the extent that such authorization or license may have an impact on the Services or on the Service Provider's rights and obligations relating to the Services, or require the Service Provider to provide additional services whether to the Province or any other Person, then the impact will be dealt with pursuant to the Change Order Process;

(d) the Service Provider will not be permitted to use the Province Proprietary Software or any Modifications thereto for the benefit of any other Person without the prior written consent of the Province, provided that the Service Provider will have the right to authorize its Subcontractors to use the Province Proprietary Software and any Modifications thereto for the purpose of providing the Services pursuant to, and in accordance with, the terms of this Agreement;

(e) the foregoing rights are granted on an "as is" basis without warranties or conditions of any kind, whether oral or written or express or implied, and the Province specifically disclaims any implied warranties or conditions of merchantability, satisfactory quality, non-infringement and fitness for a particular purpose;

(f) the foregoing rights will terminate upon expiry or termination of the Initial Term or Renewal Term, as applicable (the **"License Termination Date"**), subject to specific rights required with respect to the Termination Assistance Services; and

(g) if the Parties agree to integrate any Province Proprietary Software or Modifications thereto with any Service Provider Software, then prior to the integration thereof, the Parties will also agree upon the Service Provider's rights to use such Province Proprietary Software and Modifications thereto after the Term, and any benefits that may be granted to the Province in connection therewith.

19.6 Province License.

The Service Provider hereby grants to the Province an irrevocable, global, perpetual, assignable (for the purposes of the delivery of the Services to or by the Province or an Alternative Service Provider), non-exclusive, royalty-free, fully-paid up license and right to use the Service Provider Software that is, or at anytime hereafter may be, utilized in providing Services under this Agreement (whether notified to the Province or not). The Service Provider will provide to the Province any third party rights necessary to give effect to the foregoing. Such license includes, without limitation, the right to use, copy, maintain, modify, enhance, sublicense and create Modifications of such Service Provider Software, as well as the Source Material and related Intellectual Property upon the written request of the Province, to the extent available and possible.

19.7 Service Provider License to Modifications.

The Province hereby grants to the Service Provider an irrevocable, global, perpetual, assignable, non-exclusive, royalty-free, fully-paid up license and right to use the Modifications to the Service Provider Software. The Province will provide to the Service Provider any third party rights necessary to give effect to the foregoing. Such license includes, without limitation, the right to use, copy, maintain, modify, enhance, sublicense and create Modifications of the same, as well as the Source Material and related Intellectual Property, to the extent available and possible.

19.8 Use of Confidential Information in Licensed Rights.

The Parties agree that when one Party (the "**Licensor Party**") has granted a Software license to the other Party (the "**Licensee Party**") under this Agreement which provides the Licensee Party with any license rights to the Service Provider Software, Province Proprietary Software, or any Modifications thereto (each "**Proprietary Software**"), then the Licensee Party will be entitled to disclose or permit disclosure of that Proprietary Software, to the extent necessary and only insofar as disclosure is necessary on a needs to know basis, in order for the Licensee Party to exercise its rights under and in accordance with any licences granted by the Licensor Party to the Licensee Party under this Agreement.

19.9 Third Party Software.

In respect of any license with a third party Person (other than an Affiliate of the Service Provider, who for purposes of this Article, will be treated as the Service Provider) for Software other than "shrink wrap" or "click wrap" Software that is generally commercially available, that the Service Provider uses in providing the Services under this Agreement (the "**Third Party Software**"), the Service Provider will obtain as a provision of such license and at the time of obtaining such license (or prior to the use of such Third Party Software in providing the Services), the right to assign the license to the Province or an Alternative Service Provider without consent from, or a license transfer fee or other similar fee payable to such third party Person (and for greater clarification, excluding ordinary course ongoing license fees and maintenance costs in respect of such Third Party Software); provided that where the inclusion of such provision increases the cost of obtaining such license, then the Service Provider will be relieved of its obligation to obtain such right if it informs the Province of such increased cost (and provides the Province with detailed back-up documentation in support thereof), and the Province does not agree to be responsible for such increased cost.

19.10 Province Licensed Software.

During the Term, and subject to the other terms of this Section, the Province will:

(a) at its own expense, sublicense the Province Licensed Software to the Service Provider, or obtain a right for the Service Provider to use the Province Licensed Software, as applicable, and only to the extent required to perform the Services;

(b) at its own expense, pay all fees for maintenance and support currently subscribed for by the Province for the Province Licensed Software used or accessed by the Service Provider,

(c) not assign or otherwise dispose of the licenses relating to the Province Licensed Software or amend, or terminate the licenses and the maintenance and support arrangements for the Province Licensed Software, in all cases, in any way which would materially adversely impact the Service Provider's ability to deliver the Services; and

(d) the Province will exercise all rights of renewal under its maintenance and support arrangements in relation to the Province Licensed Software during the Term such that the current maintenance and support arrangements remain in place during the entire Term, unless otherwise determined through the Change Order Process.

Notwithstanding the foregoing, under no circumstances will the Service Provider use, or be permitted to use, any or all of the Province Licensed Software for any purpose whatsoever other than to provide the Services under the terms of this Agreement.

19.11 Third Party Notices.

If either Party receives a notice of infringement, request for disclosure, subpoena, or other inquiry with respect to any matter under this Article 19 (*Intellectual Property and Propriety Rights*), then such Party will, as soon as practical, notify the other Party in writing and the matter will be dealt with in accordance with Article 25 (*Indemnification, Liability and Guarantees*). Neither Party will respond to such notices, requests, subpoenas or inquiries, or disclose the other Party's Confidential Information to third parties, without first so notifying the other Party in writing (to the extent possible).

19.12 Intellectual Property Rights Re: New Services.

The Province and the Service Provider acknowledge that it is their intention to expand the scope of the Services in accordance with this Agreement, and recognize that, in connection with any new services, it will be necessary to reach an agreement on their respective Intellectual Property Rights in the Software that is then operated by the Province or other third parties. It is the intention of the Parties to resolve any issues associated with such Intellectual Property Rights on a basis that is consistent with the provisions of this Article 19 (*Intellectual Property and Propriety Rights*).

ARTICLE 20 – PROVINCE SHARED INFRASTRUCTURE

20.1 Ownership and Control of Province Shared Infrastructure.

The Parties acknowledge that the Service Provider requires access to and use of the Province Shared Infrastructure during all or a portion of the Term to support the delivery and performance of the Services as contemplated in this Agreement. In connection therewith, the Service Provider acknowledges that:

(a) the Province Shared Infrastructure will at all times be owned, operated and maintained by the Province or on behalf of the Province by third party Persons;

(b) the Service Provider has no ownership or other interest in the Province Shared Infrastructure other than the rights of access to, and use of, the Province Shared Infrastructure granted to the Service Provider under this Article 20 (*Province Shared Infrastructure*) for purposes of delivering and performing the Services in accordance with this Agreement; and

(c) subject to the rights of the Service Provider specifically set out in this Article 20 (*Province Shared Infrastructure*) and otherwise in this Agreement, the Province will have control of, access to and use of the Province Shared Infrastructure, and the sole control of the operation and maintenance of the Province Shared Infrastructure including changes, modifications and upgrades thereto, without requirement for consent of or Approval from the Service Provider.

20.2 Use of Province Shared Infrastructure.

The Province will make available to the Service Provider such access to and use of the Province Shared Infrastructure as is required by the Service Provider to deliver and perform the Services in accordance with this Agreement. Such access and use will be available for the period commencing on the Hand-Over Date (or commencing on such other date as may be agreed to by the Parties during the Term if access to the Province Shared Infrastructure is not required on the Hand-Over Date), to and including the end of the Termination Date, or such shorter period of use as may be required by the Service Provider (the "**Shared Infrastructure Use Period**"), and without any additional fee or payment from the Service Provider to the Province unless specifically provided otherwise in this Agreement, or through the Change Order Process. Notwithstanding the foregoing, where the Service Provider is utilizing material portions of the Province Shared Infrastructure, then the Province will advise the Service Provider by written notice of the same, and thereafter the Parties will agree, through the Change Order Process, upon a reasonable apportionment of the actual costs of the Province Shared Infrastructure and maintenance thereof that the Service Provider will pay to the Province (the "**Basic Infrastructure Credit**") in accordance with the provisions of Section 20.10 (*Basic Infrastructure Credit Payment*). If the parties are unable to agree upon the amount of the Basic Infrastructure Credit, then the determination thereof will be a Dispute and will be settled in accordance with the Dispute Resolution Process under Article 27 (*Dispute Resolution*).

20.3 Restrictions on Access and Use.

The right of the Service Provider to access and use the Province Shared Infrastructure will be subject to the following:

(a) the Service Provider will be given access to and the use of the Province Shared Infrastructure only during the normal hours of operation of the Province Shared Infrastructure during which the same is generally made available to other users thereof. The Province may change and modify such hours of operation from time to time in its discretion, and upon reasonable prior written notice to the Service Provider, provided that:

(i) the Province Shared Infrastructure will be available for use for a reasonable number of hours during each Business Day (and such non-Business Days where the Province Shared Infrastructure is ordinarily made available to its users) and at reasonable hours as may be required to support the delivery and performance of the Services,

(ii) any change or modification of the hours of operation will apply generally to users of the Province Shared Infrastructure and not only or principally to the Service Provider,

(iii) the Service Provider will not be liable for any breach of or failure to perform its obligations under this Agreement, including any failure to meet the Service Levels, to the extent that such breach or failure to perform is attributable to such change or modification of the hours of operation of the Province Share Infrastructure, and

(iv) any decrease in the hours of availability of the Province Shared Infrastructure to the Service Provider (except as may be specifically contemplated as part of the Transformation of the Services under this Agreement) will be made through the Change Order Process;

(b) in exercising its right of access to or use of the Province Shared Infrastructure, the Service Provider will:

(i) not alter, change, damage or remove any furniture, fixtures, equipment, data, information or other matter located at or comprising part of the Province Shared Infrastructure, except with the Approval of the Province, or as specifically contemplated in this Agreement or resulting from the Services provided under this Agreement, and

(ii) following each exercise of access to or use of the Province Shared Infrastructure, leave the Province Shared Infrastructure in substantially the same condition as existed prior to access to or use of the Province Shared Infrastructure by the Service Provider;

(c) the Service Provider will cause all Personnel of the Service Provider or External Personnel used by the Service Provider, in accessing or using the Province Shared Infrastructure, to:

(i) comply with all policies, rules and regulations that the Province may adopt from time to time in respect of the Province Shared Infrastructure, provided that the Province gives the Service Provider prior written notice thereof, and

(ii) at all times and in all circumstances to identify themselves as employees, agents, contractors or representatives of the Service Provider, as applicable, and not as employees, agents, contractors or representatives of the Province;

(d) the Service Provider will access and use the Province Shared Infrastructure only for the purpose of delivering and performing the Services under this Agreement, and for no additional, ancillary or other purpose unless specifically authorized in writing by the Province;

(e) the Service Provider will advise the Province of any intended reduction in use of the Province Shared Infrastructure as soon as the Service Provider is reasonably aware of the same, including any determination by the Service Provider to discontinue all or partial use of the Province Shared Infrastructure, provided that in no event is the Service Provider required to provide more than twelve months' notice of any intended reduction;

(f) to the extent that the Service Provider has any reason to believe that its use of the Province Shared Infrastructure will adversely affect the general operation of the Province Shared Infrastructure (including, without limitation, due to volume or usages changes), then the Service Provider will immediately advise the Province of the same and take all steps as directed by the Province to ensure that any adverse impact on the Province Shared Infrastructure is minimized or eliminated (recognizing that the Province uses the Province Shared Infrastructure to deliver a number of critical services within the Province, and accordingly, the minimization or elimination of any such adverse impact is paramount); and

(g) nothing in this Article 20 (*Province Shared Infrastructure*) entitles the Service Provider to require the Province to change, modify or upgrade the Province Shared Infrastructure.

20.4 Ordinary Course Changes to Province Shared Infrastructure.

The Province, in its sole discretion and from time to time, may make non-material changes, modifications, additions or upgrades to the Province Shared Infrastructure or discontinue use of any non-material portion of the Province Shared Infrastructure in the ordinary course of operations (collectively, "**Ordinary Infrastructure Changes**"), without requirement for the consent of the Service Provider and without prior notice to the Service Provider; provided that the Ordinary Infrastructure Changes do not materially affect or impact the access to and use of the Province Shared Infrastructure by the Service Provider for the delivery and performance of the Services in accordance with this Agreement. If as a result of any Ordinary Infrastructure Changes made, the Service Provider is required to change, modify or upgrade its Systems and operations in order to continue to have access to and use of the Province Shared Infrastructure, then the Service Provider will be solely responsible for making all such changes, modifications or upgrades and for all costs thereof to the Service Provider.

20.5 Material Changes to Province Shared Infrastructure.

The Province may make material changes, modifications, additions or upgrades to the Province Shared Infrastructure or discontinue use of any material portion of the Province Shared Infrastructure from time to time (the "**Material Infrastructure Change**"), notwithstanding that the Material Infrastructure Change may have a material adverse effect or impact on the access to and use of the Province Shared Infrastructure by the Service Provider, provided that:

(a) subject to the Service Provider implementing any changes, modifications, additions or upgrades to its Systems and operations as contemplated in this Section, the Service Provider will continue to have access to and use of the Province Shared Infrastructure to the extent that the Province Shared Infrastructure continues to be operated by the Province; and

(b) the Province will give reasonable prior written notice to the Service Provider of the details of the Material Infrastructure Change, including the analysis of the Province as to the effect and impact of the Material Infrastructure Change to the Service Provider, to the extent known, in the delivery and performance of the Services pursuant to this Agreement.

Where a Material Infrastructure Change may be reasonably expected to have a material adverse effect or impact on the Service Provider, the Province will provide the notice of the Material Infrastructure Change to the Service Provider sufficiently in advance of the implementation thereof so as to afford the Service Provider a reasonable opportunity to make the required changes, modifications, additions and upgrades to its Systems and operations prior to such implementation. The Service Provider will be solely responsible

for making all such required changes, modifications and upgrades that may be required as a result of the Material Infrastructure Change, and any material adverse impact suffered or incurred by the Service Provider as a result thereof will be addressed by the Parties through the Governance Process or the Change order Process. For greater clarification, the Province may discontinue use of any portion of the Province Shared Infrastructure pursuant to this Section where any managed applications of the Service Provider running on the Province Shared Infrastructure cause process loops, runaway jobs, extreme load conditions or other similar adverse impacts to users of the Province Shared Infrastructure, in which case any material adverse impact suffered or incurred by the Service Provider in respect thereof will be at the sole cost of the Service Provider, and will not be addressed by the parties pursuant to the Governance Process or the Change Order Process.

20.6 Changes Required for or Initiated by the Service Provider.

Where a change to the Province Shared Infrastructure is required for the continued access to and use of the Province Shared Infrastructure by the Service Provider (such as a change to accommodate increased demand or capacity required by the Service Provider or to accommodate a change in the Systems and operations of the Service Provider), or is requested or initiated by the Service Provider, then the following will apply:

(a) the Service Provider may request a change to be made to the Province Shared Infrastructure by notice in writing to the Province which notice will include a detailed description of all business and technical requirements relating to such requested change, to the extent known;

(b) the Province will review and consider any change to the Province Shared Infrastructure as may be reasonably requested by the Service Provider from time to time, having regard to all of the surrounding circumstances including, without limitation, the impact on and the interests of the other users of the Province Shared Infrastructure, and will implement any such changes as may be Approved by the Province;

(c) unless the Service Provider has given notice to the Province that the Service Provider will prepare the plan for the implementation of any such required or requested change, the Province will, at the cost of the Service Provider, prepare a plan for such change and will provide such plan to the Service Provider for its review and consideration;

(d) the plan for the implementation of any such required or requested change will include a detailed description of each change to the Province Shared Infrastructure proposed to be made, as well as a budget of costs anticipated to be incurred to effect and implement such change, and a forecast of any increase to the operating and maintenance costs of the Province in respect of the Province Shared Infrastructure as a result from such change, all to the extent known or reasonably anticipated;

(e) the Province will incorporate all reasonable comments and suggestions as the Service Provider may provide to the Province in writing provided that, for greater clarification, the Province will, at all times, have and retain the sole right to determine the appropriate plan and actions to implement such required or requested change and will have the right to grant the final Approval thereof;

(f) if the Service Provider does not agree with the proposed plan or implementation of the proposed change to the Province Shared Infrastructure, or of the estimated costs or forecast thereof as provided by the Province to the Service Provider, then matter will be

deemed to be a Dispute and will be settled in accordance with the Dispute Resolution Process under Article 27 (*Dispute Resolution*); and

(g) notwithstanding the foregoing, and for greater clarification, the Province will not require the Approval of the Service Provider to the plan in respect of or the implementation of any such required or requested change to the Province Shared Infrastructure and may proceed with such plan and the implementation of such change notwithstanding initiation by the Service Provider of a Dispute pursuant to paragraph (f) above.

20.7 Cooperation of the Parties.

The Parties will cooperate with each other and will use reasonable efforts to make and implement any change, modification or upgrade to the Province Shared Infrastructure determined or Approved by the Province contemplated in this Article 20 (*Province Shared Infrastructure*), including testing of such change, modification or upgrade.

20.8 Change Order Process.

Unless specifically provided otherwise in this Article 20 (*Province Shared Infrastructure*), the change process set forth in Section 20.6 (*Changes Required or Initiated by Service Provider*), is in lieu of the Change Order Process with respect to the Province Shared Infrastructure.

20.9 Failure of Province Shared Infrastructure.

In the event of an unanticipated failure of the Province Shared Infrastructure, or the occurrence of any unanticipated event or circumstance which prevents the Service Provider from having access to and use of the Province Shared Infrastructure, as is required by the Service Provider for the delivery and performance of the Services, whether arising from the negligence or fault of the Province or otherwise, the Province and the Service Provider acknowledge and agree that:

(a) the Province will have no liability or obligation to the Service Provider in respect thereof other than the obligation to use reasonable efforts and to act with due diligence to correct such failure, or to restore such access to and use of, the Province Shared Infrastructure as soon as reasonably practicable; and

(b) to the extent that the Service Provider is not able to deliver or perform a Service in the manner or to the Service Level required under this Agreement, or to perform any other obligations under this Agreement, as a result of such failure or lack of access to or use of the Province Shared Infrastructure, the Service Provider will be released of all consequences otherwise provided in this Agreement in respect of such failure to deliver and perform such Service, to meet such applicable Service Level or to perform such obligations under this Agreement, until such failure or lack of access to or use of the Province Shared Infrastructure is rectified or remedied to a degree that the Service Provider is able to deliver and perform the Services, and to perform its obligations in accordance with this Agreement.

20.10 Basic Infrastructure Credit Payment.

Where the Service Provider is required by this Article 20 (*Province Shared Infrastructure*) to pay to the Province a Basic Infrastructure Credit or any other payment relating to the Province Shared Infrastructure, then the following provisions will apply:

(a) the Service Provider will make such payment by recording, in favour of the Province, a credit against the Fees payable to the Service Provider under this Agreement, which credit will be applied on a monthly basis, to the extent applicable;

(b) the Province may, at any time, direct the Service Provider not to record a Shared Infrastructure Credit in favour of the Province in respect of an amount payable by the Service Provider to the Province pursuant to this Article 20 (*Province Shared Infrastructure*), and instead to pay such amount to a third party as may be designated by the Province, in which event, the Service Provider will pay such amount to the third party as directed by the Province, and will not record such amount as a credit in favour of the Province. In such event, receipt of payment of such amount by the third party will, and will be deemed to be, receipt of payment of the amount by the Province for all purposes of this Agreement; and

(c) if the Service Provider fails to comply with the preceding provisions of this Section in respect of an amount payable by the Service Provider to the Province under this Article 20 (*Province Shared Infrastructure*), the Province may, by notice in writing to the Service Provider, set-off such amount payable by the Service Provider against any Fees payable by the province to the Service Provider under this Agreement.

20.11 Indemnity.

Notwithstanding any other provision contained in this Article 20 (*Province Shared Infrastructure*), and in addition to any other indemnities provided by the Service Provider to the Province pursuant to this Agreement, the Service Provider hereby indemnifies and agrees to hold harmless the Province and its employees, agents and representatives, to the fullest extent permitted by law, from and against any and all Claims suffered or incurred by any of them arising out of or in connection with the access to and use of the Province Shared Infrastructure by the Service Provider.

20.12 Termination of Rights to Province Shared Infrastructure.

The Service Provider acknowledges and agrees that its rights in respect of the Province Shared Infrastructure under this Article 20 (*Province Shared Infrastructure*) will cease upon the expiry (or earlier termination in accordance with this Article 20 (*Province Shared Infrastructure*)) of the Shared Infrastructure Use Period. Upon such expiry, the Service Provider will return to the Province all passwords, access codes, access cards and devices of any kind used to obtain access to and use of the Province Shared Infrastructure. For greater clarification, if the Province discontinues use of any portion of the Province Shared Infrastructure, then upon the discontinuance thereof the Service Provider's rights in respect of the discontinued portion of the Province Shared Infrastructure under this Article 20 (*Province Shared Infrastructure*) will cease, and the Service Provider will return to the Province all passwords, access codes, access cards and devices of any kind used to obtain access to and use of the discontinued portion of the Province Shared Infrastructure.

ARTICLE 21 – OTHER COMMERCIAL TERMS

21.1 Growth and Marketing.

The Parties will market and otherwise deal with any customers of the Services and the Stakeholders, and will otherwise undertake growth and marketing activities in respect of the Services, in accordance with **Schedule 26** *(Growth and Marketing)*.

21.2 Gainsharing.

The Parties will comply with, and hereby agree to, the gainsharing provisions and principles set forth in the attached **Schedule 27** *(Gainsharing)*.

ARTICLE 22 – AUDIT RIGHTS

22.1 Access Rights.

During the Term, and for a period of seven (7) years after the end of the Term, upon prior written request of the Province, except where such prior notice is not required pursuant to the express provisions of this Article 22 (*Audit Rights*) or any other express provisions of this Agreement, the Service Provider will provide the Province and its auditors and other authorized representatives of the Province with access to the following including, where applicable and practicable to do so, with electronic access, to:

(a) all the Province Records or Personal Information related to the Services then in the Custody of the Service Provider, wherever maintained;

(b) any System that contains such Province Records or Personal Information related to the Services, wherever maintained; and

(c) any property or facility at which the Services are being performed, where any such Systems are housed, or where any such Province Records or Personal Information are maintained or stored.

The provisions of Section 22.7 (*General Principles*) will apply with respect to the access rights granted to the Province under this Section.

22.2 Examinations and Copies.

During the Term, upon the prior written request of the Province, the Service Provider will permit the Province and its auditors and their respective authorized representatives, during business hours, to examine and make copies of any computer-stored data, correspondence, accounting procedures and practices, and any other relevant supporting financial or operational data including, without limitation, invoices, payments, claims and receipts, and in all cases pertaining to the Services, which will be made available by the Service Provider to the Province and its auditors, and their respective authorized representatives, in British Columbia. Both Parties acknowledge and agree that nothing in this Section will in any way limit or restrict the confidentiality obligations as set forth in Article 16 (*Privacy, Security and Confidentiality*) or as otherwise contemplated by this Agreement.

22.3 Inspection and Investigation Rights.

In the event of a breach or a perceived breach of this Agreement, the Province will have the right, at any time and without prior notice to the Service Provider, either directly or through its representatives, to inspect all or any matters in respect of the Services performed by or on behalf of the Service Provider under this Agreement, and to perform investigations in respect of any matter of concern to the Province or any matter which the Province otherwise becomes aware of in connection with the Services under this Agreement. The Province will make reasonable efforts in exercising such right of inspection or investigation to not hinder or interfere with the performance of the Services by the Service Provider under this Agreement. For greater clarification, the Province acknowledges that to the extent that any such exercise of the Province's right of inspection or investigation directly hinders or interferes with the Service Provider's ability to deliver Services under this Agreement, then the Service Provider will not be

responsible for any Service failure resulting therefrom. The Service Provider will provide the Province and its representatives with all reasonable assistance in connection with any such inspections and investigations. The provisions of Section 22.7 (*General Principles*) will apply with respect to the inspection or investigation rights granted to the Province hereunder.

22.4 Audit Rights.

The Province may appoint an internal or external auditor or other professional advisor at any time and from time to time, but subject to the provisions of 22.7 *(General Principles)*, to review and confirm or verify, in respect of any Contract Year, any aspect of this Agreement and the Services performed under this Agreement including, without limitation, the following:

(a) any matter related to the operational aspects of this Agreement and the Services including, without limitation, to certify or verify:

(i) the integrity of the Province Records or Province Confidential Information including, without limitation, the completeness, accuracy, timelines, confidentiality, availability and security in respect thereof;

(ii) the privacy and security processes of the Service Provider and its Access Subcontractors, and the compliance of the Service Provider and its Access Subcontractors with the Privacy Obligations;

(iii) the general controls, practices, and procedures utilized by the Service Provider in connection with the Services performed;

(iv) the stability and security of the Systems and processes utilized by the Service Provider in performing the Services;

(v) the integrity of all reports provided by the Service Provider to the Province (including the raw data from which such reports are compiled);

(vi) that the Services are being provided in accordance with the terms of this Agreement (including the Service Levels), and in accordance with all Applicable Laws, the Province Policies and any applicable requirements of any regulatory body or authority having competent jurisdiction; and

(vii) the reviews and audits referred to in Article 17 (*Business Continuity and Disaster Recovery*) in respect of the Business Continuity Plan and Disaster Recovery Plan;

(b) any matter related to the financial or business aspects of this Agreement, including verifying the accuracy of all Fees or other amounts invoiced to, or paid by, the Province, the accuracy of financial information provided by the Service Provider to the Province in respect of the calculation of Fees or other amounts invoiced to the Province or set forth in any Proposal in connection with the Change Order Process, or any credits or reductions against the Fees (whether or not properly granted as required by the Service Provider to the Province), and the accuracy of any reporting by the Service Provider to the Province in connection with the foregoing;

(c) operational and other audits requested or otherwise required to be undertaken by the Office of the Comptroller General or the Office of the Auditor General of the Province

under the *Financial Administration Act* or any other Applicable Laws regarding any aspect of this Agreement (including, without limitation, an audit of the compliance by the Service Provider with the requirements of this Agreement), or any audits that may be required by Cabinet or Treasury Board of the Province; or

(d) such other audits relating to this Agreement, the obligations of the Service Provider under this Agreement, or the Services as the Province may determine from time to time.

For greater clarification, the Province may, in connection with the exercise of its audit rights pursuant to this Section 22.4 (*Audit Rights*), exercise or cause the Service Provider to exercise rights in respect in this Section.

22.5 Costs.

The costs of any inspections, investigations and audits will be dealt with in accordance with the following provisions:

(a) except as set forth in paragraph (b) below, the Province will pay its costs and expenses of any investigations and inspections under Section 22.3 (*Inspection and Investigation Rights*), and the costs and expenses of any auditor or other professional advisor retained by the Province to conduct or assist with an audit under Section 22.4 (*Audit Rights*) or Section 22.6 (*SysTrust Report*). The Service Provider will pay, and will not seek reimbursement from the Province, for the Service Provider's (or its Subcontractors') costs incurred in connection with any inspection or investigation under Section 22.3 (*Inspection and Investigation Rights*), or any audit conducted pursuant to Section 22.4 (*Audit Rights*) or Section 22.6 (*SysTrust Report*), including the cost of the time and effort of the Service Provider and its Personnel, Subcontractors and External Personnel to comply with the requests and requirements of an inspector, investigator, auditor or other professional advisor in respect of the same; and

(b) where an investigation, inspection or audit reveals a material Deficiency (as determined by the Province, acting reasonably) as a result of the acts or omissions of the Service Provider (or of those Persons for whom the Service Provider is responsible at law or pursuant to the terms of this Agreement), the costs of such inspection, investigation or audit, including the costs of other professional advisors retained by the Province to conduct the same, will, at the option of the Province, be paid by the Service Provider, in which case the following provisions will apply:

(i) such costs will not be recovered from or reimbursed by the Province to the Service Provider,

(ii) if any such costs are paid by the Province, then the Province will be entitled to reimbursement of such costs from the Service Provider, or to set-off such costs against the Fees otherwise payable to the Service Provider,

(iii) any such costs payable by the Service Provider will be payable upon receipt by the Service Provider of an invoice from the Province in respect of such costs, and

(iv) upon correction of the material Deficiency so identified, and if so requested by the Province, the Service Provider will undertake a new audit, at the Service Provider's expense, to confirm that such material Deficiency has been fully

addressed and remedied. The Service Provider will promptly provide the results of such audit to the Province upon the Service Provider's receipt of the same.

22.6 SysTrust Report.

The Province may from time to time conduct a "Trust Services Principles and Criteria" examination as governed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (the "**SysTrust Report**") in respect of the Services being provided under this Agreement. The SysTrust Report will report on controls throughout a Contract Year. The SysTrust Report will be deemed to be an audit for the purposes of this Article 22 (*Audit Rights*) with costs, Deficiency correction and all other matters addressed in the manner as set forth in this Article 22 (*Audit Rights*) for audits.

22.7 General Principles.

In connection with the access, inspection, investigation and audit rights granted to the Province and other Persons under this Article 22 (*Audit Rights*):

(a) the auditors, investigators, inspectors or representatives of the Province will be qualified and trained to levels appropriate to conduct audits, inspections or investigations being conducted;

(b) the Province will cause all such audits, inspections and investigations to be performed during the normal business hours for the Services in question, and upon reasonable prior notice to the Service Provider, other than for inspections or investigations pursuant to Section 22.3 (*Inspection and Investigation Rights*) which may be performed at any time without notice;

(c) the Province will, and will cause its auditors, investigators, inspectors or representatives to:

(i) use reasonable efforts not to hinder or interfere with the performance of the Services by the Service Provider, and for greater clarification, the Province acknowledges that to the extent any such exercise of rights directly hinders or interferes with the Service Provider's ability to deliver the Services, then the Service Provider will not be responsible for any resulting Service Level failures in respect thereof, and

(ii) comply with all security and other similar policies of the Service Provider while at its premises, provided that the Service Provider provides the Province with reasonable prior notice thereof, and provided further that any such security or other similar polices of the Service Provider do not unduly hinder or interfere with the conduct of the audit, inspection or investigation in question;

(d) the Service Provider will, and will cause its Personnel, Subcontractors and External Personnel to:

(i) cooperate with any such inspections, investigations and audits performed by the Province through the Province's auditors, investigators, inspectors or representatives,

(ii) make available on a timely basis the information and Records requested by the Province or its auditors, investigators, inspectors or representatives, and

(iii) provide the Province and its auditors, investigators, inspectors or representatives with assistance in obtaining access to such information and Records, and to any Subcontractors, Personnel or External Personnel, as may be reasonably requested;

(e) the access rights provided for with respect to the premises of the Service Provider will also extend to those premises at which Province Confidential Information, Province Records or Personal Information is stored, and the Service Provider will obtain such corresponding rights from its Subcontractors as may be necessary to give effect to this provision; and

(f) the Service Provider will be given the opportunity to respond to the audit, inspection or investigation results before they are finalized, except where it is not reasonably possible or appropriate, as determined by the Province.

22.8 Deficiencies.

Following delivery to the Service Provider of an audit, inspection or investigation report that outlines accounting or other Deficiencies of the Service Provider, the Parties will meet as soon as possible through the Governance Process in order to discuss and resolve such Deficiencies. In connection therewith, the following provisions will apply:

(a) if the report identifies the potential for any Deficiency, then the Service Provider will provide the Province, through the Governance Process, with the Service Provider's assessment of the impact of the potential Deficiency;

(b) subject to any alternative agreement reached between the Parties through the Governance Process, the Service Provider will, as soon as reasonably possible (but in any event within thirty (30) days), develop and present to the Province, through the Governance Process, a corrective action plan outlining the timely corrective action that has been taken, or will be taken, by the Service Provider to remedy the Deficiencies;

(c) the corrective action plan will include a sufficient level of detail to allow the Province to assess the appropriateness of the corrective action and plan, including a description of the Deficiency, the specific action to be taken, and a specific implementation schedule that specifies dates and Persons responsible for taking, or who have already taken, the corrective action;

(d) the Province will be given the opportunity, through the Governance Process, to provide the Service Provider with any comments that the Province may have on the corrective action plan, and the Service Provider will take all such comments received by the Province into consideration; and

(e) the Service Provider will remedy the Deficiencies in accordance with the corrective action plan, provided that the Service Provider will be entitled to remedy any Deficiencies that that are not material in nature, or that do not involve access, use or disclosure of Personal Information, in the ordinary course of business.

ARTICLE 23 – GENERAL DUTIES AND OBLIGATIONS

23.1 General Duties and Obligations of Service Provider.

At all times during the Term and without limiting the other provisions set forth in this Agreement, the Service Provider agrees to, and to cause its directors, officers, Personnel, Affiliates, Subcontractors and all External Personnel to, perform its obligations under this Agreement and to deliver the Services as follows:

(a) in compliance with all of the terms and conditions of this Agreement and all other documents referenced in this Agreement;

(b) in a manner that is consistent with the Parties' objectives set out in Section 1.13 (*Objectives of the Parties*);

(c) in accordance with the standard of care set forth in Section 4.4 (*Standard of Care*);

(d) in accordance with any Change Orders and any agreements made between the Parties pursuant to the Governance Process;

(e) in compliance with all applicable Province Policies which have been provided or otherwise communicated by the Province to the Service Provider from time to time, and in accordance with the Change Order Process; and

(f) in compliance with all Applicable Laws.

23.2 Compliance with Specific Laws.

Without limiting the foregoing Section 23.1 (*General Duties and Obligations of Service Provider*), at all times during the Term, and in the performance of the Services under this Agreement, the Service Provider will comply with, and will cause its Personnel and its Subcontractors and their External Personnel to comply with, those specific Applicable Laws set forth in **Schedule 28** *(Specific Laws and Policies)*, and any other specific Applicable Laws not listed in **Schedule 28** *(Specific Laws and Policies)* but which otherwise apply to the Services given the nature thereof, or any applicable regulations or standards governing the particular industry to which the Services relate. The Service Provider acknowledges that it is familiar with the foregoing as they apply to the Service Provider or to the Services, as applicable.

23.3 FOIPPA Inspections.

The Service Provider acknowledges that under the *Freedom of Information and Protection of Privacy Act* (British Columbia), the Commissioner has the power to obtain information and evidence from persons other than the Province in the course of conducting an investigation or an inquiry under that Act. Accordingly, the Service Provider will cooperate with respect to investigations or inquiries of the Commissioner under that Act regarding Province or Personal Information related matters, and in respect of any information to which the Commissioner is entitled to under such Act.

23.4 Licenses and Permits.

At all times during the Term, the Service Provider will, at its own cost, obtain and maintain in full force and effect all licenses and permits issued by any Governmental Authority which are required or desirable for the proper performance of the Services, or otherwise required or desirable for the performance and completion of the transactions contemplated in this Agreement.

ARTICLE 24 – REPRESENTATIONS, WARRANTIES AND COVENANTS

24.1 Province Representations and Warranties.

The Province represents, warrants and covenants as follows to the Service Provider, as of the date of this Agreement and throughout the Term, and acknowledges and confirms that the Service Provider is relying upon such representations, warranties and covenants in entering into this Agreement:

(a) the Province has the power and authority to enter into, execute and deliver this Agreement and the other Transaction Documents, which have been duly executed and delivered by the Province, and each constitutes a legal, valid and binding obligation of the Province enforceable against it in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunction are equitable remedies available only in the discretion of the court;

(b) the Province has the power and authority to perform its obligations under this Agreement and the other Transaction Documents as contemplated in this Agreement; and

(c) neither the execution and delivery of this Agreement, the other Transaction Documents, nor the compliance with the terms thereof by the Province:

(i) has resulted or will result in a violation of any Applicable Laws, or

(ii) requires the Approval or consent of any Person or any Governmental Authority except such as has been obtained as of the date of this Agreement.

24.2 Service Provider Representations, Warranties and Covenants.

The Service Provider represents, warrants and covenants as follows to the Province, as of the date of this Agreement and (except as otherwise noted) throughout the Term, and acknowledges and confirms that the Province is relying upon such representations, warranties and covenants in entering into of this Agreement:

Corporate Existence and Structure

(a) the Service Provider is a corporation duly incorporated and validly existing under the laws of **[insert jurisdiction of incorporation]** and is in good standing with respect to the filing of annual returns thereunder;

(b) all of the issued and outstanding shares in the capital of the Service Provider are registered in the name of the Performance Guarantor, and the Performance Guarantor is the legal and beneficial owner thereof **[NOTE – amend as necessary but ensure that the Service Provider is a Canadian Entity, owned by a Canadian Entity]**;

(c) the Performance Guarantor is a company duly incorporated and validly existing under the laws of **[insert jurisdiction of incorporation]** and is in good standing with respect to the filing of annual returns thereunder;

(d) all of the issued and outstanding shares in the capital of the Performance Guarantor are registered in the name of **[insert name of Canadian Entity]**, being a Canadian Entity and the legal and beneficial owner of such shares **[NOTE – amend as necessary but**

ensure that the Performance Guarantor is a Canadian Entity, owned by a Canadian Entity];

(e) the Financial Guarantor is a publicly-held company **[amend if incorrect]** duly incorporated and validly existing under the laws of **[insert jurisdiction of incorporation]** and listed on the **[insert name of Stock Exchange, and if not publicly trading, then insert good standing representation];**

(f) the Service Provider has, and throughout the Term will maintain, its registered office within the Province of British Columbia; **[NOTE - if the Service Provider is not a BC company, or if it is a federal company with its registered office outside of BC, then change to an extra-provincial registration representation]**

(g) the majority of the Service Provider's directors are resident in Canada;

Power, Capacity and Legal Authority

(h) the Service Provider has all necessary corporate power, capacity and legal authority to enter into, execute and deliver this Agreement and the Transaction Documents to which it is a party, and to perform its obligations under this Agreement and such Transaction Documents, and this Agreement and such Transaction Documents have been duly executed and delivered by the Service Provider, and each constitutes a legal, valid and binding obligation of the Service Provider enforceable against the Service Provider in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

(i) the Performance Guarantor has all necessary corporate power, capacity and legal authority to enter into, execute and deliver the Performance Guarantee and to perform its obligations thereunder, and the Performance Guarantee has been duly executed and delivered by the Performance Guarantor, and constitutes a legal, valid and binding obligation of the Performance Guarantor enforceable against the Performance Guarantor in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

(j) the Financial Guarantor has all necessary corporate power, capacity and legal authority to enter into, execute and deliver the Financial Guarantee and to perform its obligations thereunder, and the Financial Guarantee has been duly executed and delivered by the Financial Guarantor, and constitutes a legal, valid and binding obligation of the Financial Guarantor enforceable against the Financial Guarantor in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

No Violation

(k) neither the execution and delivery of this Agreement and the other Transaction Documents, nor the compliance with the terms of this Agreement and the other Transaction Documents by the Service Provider:

(i) has resulted or will result in a violation of any Applicable Laws,

(ii) has resulted or will result in a breach of, or constitute a default under, the Service Provider's constating documents, any shareholders' agreement to which it is a party, or any shareholder or directors' resolutions,

(iii) has resulted or will result in a breach of, or constitute a default under, any instrument or agreement to which the Service Provider is a party or by which the Service Provider is bound, or

(iv) requires the Approval or any consent of any Person or any Governmental Authority except such as has been obtained as of the date of this Agreement;

Permits, Approvals and Operating Matters

(l) the Service Provider holds, and will hold as of the Hand-Over Date and throughout the Term, all material permits, approvals, authorizations and consents that may be required from any Person or Governmental Authority in order for the Service Provider to perform its duties and obligations pursuant to the terms of this Agreement and to provide the Services as contemplated under this Agreement, and the Service Provider is, and at the Hand-Over Date and throughout the Term will be, in good standing with respect to all such permits, approvals, authorizations and consents, and none of the same contain, or will contain, any term, provision, condition or limitation which would have a material adverse effect on, or materially adversely restrict or impair the performance by, the Service Provider of its duties and obligations under this Agreement or the performance of the Services pursuant to the terms of this Agreement;

(m) the Service Provider has filed all tax, corporate information and other returns required to be filed under all Applicable Laws, has complied with all workers compensation legislation and other similar legislation to which it may be subject, and has paid all Taxes, fees and assessments calculated to be due by it under those laws as of the date of this Agreement;

(n) the Service Provider has, and throughout the Term will maintain, sufficient and appropriate assets and Personnel to enable the Service Provider to perform and fulfill its obligations under this Agreement and to perform the Services in accordance with the terms of this Agreement;

Intellectual Property, Systems and Assets

(o) the performance by the Service Provider of the Services under this Agreement, and all of the Systems, Software and other Intellectual Property utilized by the Service Provider in the delivery of the Services (other than Intellectual Property licensed by the Province to the Service Provider pursuant to Section 19.5 (*Use of Province Software for the Services*)) does not and will not violate or infringe, or constitute a misappropriation of, the Intellectual Property or rights of any Person;

(p) all Systems used by the Service Provider or its Subcontractors will be maintained by the Service Provider or its Subcontractors in good working order, ordinary wear and tear excepted;

(q) all tangible personal assets including hardware that are transferred, assigned or licensed (as applicable in accordance with the terms of this Agreement) by the Service Provider to the Province at any time during the Term and upon the Termination, will be free and clear of all Liens at the time of transfer, assignment or license to the Province, other than the interests of a lessor in respect of any leased assets, or such Liens as may have been granted in respect of such leased assets by the lessor thereof;

(r) at such time as the Service Provider transfers, assigns or licenses any Intellectual Property or Intellectual Property Rights to the Province pursuant to this Agreement, the Service Provider will have all necessary right, title and interest in the Intellectual Property or Intellectual Property Rights to complete such transfer, assignment or license, as the case may be, in accordance with its terms;

Litigation, Proceedings and Limiting Agreements

(s) as of date of this Agreement, there are no suits, actions, proceedings, judgments or orders outstanding or, to the knowledge of the Service Provider, threatened against or affecting the Service Provider or any of its assets by or before any court, tribunal, board or other Governmental Authority that would, if adversely determined, have a material adverse effect on, or materially adversely restrict or impair the performance by, the Service Provider of its duties and obligations under this Agreement or the performance of the Services pursuant to the terms of this Agreement;

(t) as of the date of this Agreement, there are no material labour actions, proceedings, grievances, judgments or orders outstanding or, to the knowledge of the Service Provider, threatened against or affecting the Service Provider by or before any court, tribunal, board or other Governmental Authority, which could have a material adverse effect on, or materially adversely restrict or impair the performance by, the Service Provider of its duties and obligations under this Agreement or the performance of the Services pursuant to the terms of this Agreement;

Insolvency

(u) the Service Provider is not insolvent, is able to pay its debts as they become due in the ordinary course of business, and the entering into of this Agreement and the other Transaction Documents and the performing of its obligations under this Agreement and the other Transaction Documents will not render the Service Provider insolvent or unable to pay its debts as they become due;

Subcontractors and Personnel

(v) attached as **Schedule 20** *(Subcontractor Matters)* is a list of all of the Subcontractors who are required to be Approved by the Province under the provisions of Section 12.11 (*Consent to Use of Material Subcontractors*) with respect to the performance of the Services, as such Schedule may be amended from time to time in order to accurately reflect such Subcontractors during the Term, and all other actions required to be taken with respect to such Subcontractors have been taken including, without limitation, the incorporation in the agreements with such Subcontractors of the required provisions as set forth in Article 12 (*Subcontractors*) and in the Privacy Obligations;

Miscellaneous

(w) all information provided by the Service Provider to the Province in the course of responding to the JSRFP prior to entering into this Agreement was true and correct in all material respects and was not intentionally misleading at the time of disclosure, and the Service Provider has not intentionally failed to disclose any further information which failure would make the information previously disclosed misleading;

(x) the Service Provider is under no current obligation or restriction, nor will it knowingly assume any such obligation or restriction that does or could in any way interfere or conflict with, or that does or could present a conflict of interest concerning, the performance of the Service Provider's obligations and the providing of the Services under the terms of this Agreement;

(y) there has been no collusion, relationship with, benefit granted to or benefit received from any other Person with respect to the JSRFP, this Agreement, the delivery of the Services or anything related thereto except:

(i) for subcontracts, teaming agreements and other similar contracts entered into in the ordinary course of business,

(ii) obligations to pay commissions or other incentive compensation in compliance with compensations programs of the Service Provider and its Subcontractors and its or their Affiliates, and

(iii) as otherwise expressly disclosed by the Service Provider to the Province in writing;

(z) the Service Provider has no knowledge of any material fact or matter not disclosed to the Province by the Service Provider which, if known by the Province, might be reasonably expected to deter the Province from entering into this Agreement or completing the transactions contemplated in this Agreement and in the other Transaction Documents, or that might materially adversely affect the ability of the Service Provider to perform its obligations under this Agreement; and

(aa) the Service provider represents and warrants those matter specifically set forth in **Schedule 29** *(Additional Representations and Warranties)*.

24.3 Disclaimer of Warranties.

Other than the representations and warranties expressly set out in this Agreement or in the other Transaction Documents, neither Party makes any representation or warranty, expressed, implied, statutory or otherwise regarding any matter in connection with this Agreement or the other Transaction Documents including representations or warranties of merchantability or fitness for a particular purpose.

24.4 No Guarantee of Service Volumes.

The Service Provider acknowledges and agrees that the Province makes no representation or warranty as to the nature, timing, quality, quantity or volume of Services required from the Service Provider under this Agreement, or the volume of business or any particular type of transaction or other measurable matter that will be handled by the Service Provider in providing the Services under this Agreement, or the compensation that may be earned by the Service Provider under this Agreement. The Service Provider

acknowledges and agrees that it has conducted its own due diligence prior to entering into this Agreement as to the services performed by or on behalf of the Province historically in connection with the business that will be undertaken by the Service Provider in performing the Services. The Province has advised the Service Provider, and the Service Provider acknowledges, that historic information with respect to the Services or such business, including any particular type of transaction or other measurable matter, may not be representative of the future nature, timing, quality, quantity or volume of Services that will be required under or performed by the Service Provider under this Agreement, or the volume of business or any particular type of transaction or other measurable matter that will be handled by the Service Provider in connection with this Agreement.

ARTICLE 25 – INDEMNIFICATION, LIABILITY AND GUARANTEES

25.1 General Intent.

Each Party will be liable to the other for any damages that may be properly and lawfully awarded against each Party in favour of the other under the terms of, or in connection with, this Agreement. Both Parties agree, however, that monetary damages may not be a sufficient remedy for any breach of this Agreement, and each Party will be entitled to seek equitable relief, including injunctive relief and specific performance in the event of a breach of this Agreement, to the extent that such remedy is available to a Party in accordance with Applicable Laws (including, without limitation, the *Crown Proceeding Act* (British Columbia)), but subject any express limitations otherwise provided for in this Agreement.

25.2 Indemnification by the Service Provider.

The Service Provider will indemnify and save harmless the Province and its employees, advisors, agents and representatives (the "**Province Indemnified Parties**"), to the fullest extent permitted by law, from and against any Claims that may be suffered or incurred by any one or more of the Province Indemnified Parties arising as a result of, or in connection with, any of the matters set forth in **Schedule 30** *(Indemnification Matters)*, except to the extent suffered or incurred as a result of or in connection with the wilful misconduct, fraud, malfeasance or gross negligence of the Province Indemnified Parties.

25.3 Third Party Claim Process.

Subject to any restrictions or other limitations contained in the *Crown Proceeding Act* (British Columbia), or other Applicable Laws:

(a) if a Party (an "**Indemnified Party**") intends to seek indemnification under this Agreement from the other Party (the "**Indemnifying Party**") in respect of any third party Claims, then the Indemnified Party will promptly give the Indemnifying Party written notice of such Claims for indemnification, such notice to be given as soon as practicable following the commencement of any action by a third party; provided, however, that the failure of an Indemnified Party to give the Indemnifying Party such prompt notice will not relieve the Indemnifying Party of its obligations under this Agreement, except to the extent that such failure results in a material prejudice to the Indemnifying Party's defence to such Claims;

(b) if the Indemnifying Party receives a notice of any Claims pursuant to paragraph (a) above, then:

(i) where the Indemnifying Party is the Province, it will have the right to assume the defence of such Claims, at its sole cost and expense, with counsel designated by the Province; and

(ii) where the Indemnifying Party is the Service Provider, the Province will cooperate with the Service Provider and, where appropriate and in the discretion of the Province, will allow the Service Provider to control the defence of the Claim and any related settlement, at the Service Provider's sole cost and expense, it being acknowledged and agreed that where the Province determines that it is not so appropriate, then the Province will control the defence of the Claim and any related settlement;

provided, however, that if the defendants in any such action include both the Indemnified Party and the Indemnifying Party, and the Indemnified Party reasonably concludes that there may be legal defences available to it which are different from or additional to those available to the Indemnifying Party, then the Indemnified Party will have the right to select separate counsel, the cost of which will be at the Indemnified Party's expense (without reimbursement by the Indemnifying Party under an indemnity or otherwise) to assert such legal defences or to otherwise participate in the defence of such action on behalf of the Indemnified Party;

(c) if the Indemnified Party is entitled to indemnification under this Agreement as a result of a Claim by a third party, and if the Indemnifying Party fails or chooses not to assume the defence of such Claim, or fails to proceed, then the Indemnified Party may, at the expense of the Indemnifying Party, contest (or, with or without the prior consent of the Indemnifying Party, settle) such Claim. The Indemnified Party will not otherwise settle any Claim with respect to which it has sought or intends to seek indemnification pursuant to this Agreement without the prior written consent of the Indemnifying Party, which consent will not be unreasonably withheld or delayed; and

(d) if the Indemnifying Party settles any Claims that it may be liable to provide indemnification pursuant to this Section without the prior written consent of the Indemnified Party, which consent will not be unreasonably withheld or delayed (acknowledging that pursuant to the *Crown Proceeding Act* (British Columbia) the Province is not required to obtain or provide such consent, and will not be required to do so pursuant to this provision); then if the Indemnifying Party has reached a *bona fide* full and final settlement in respect of all Claims involving the Indemnified Party and such plaintiff(s) in any such action with the plaintiff(s), and the Indemnified Party does not (or is not asked to) consent to such settlement, the dollar amount specified in the settlement will act as an absolute maximum limit on the indemnification obligation of the Indemnifying Party.

25.4 Mitigation.

Each Party has a duty to mitigate the Claims that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and reasonable actions to reduce or limit the amount of such Claims.

25.5 Limitation on Liability.

The liability of the Parties under this Agreement will be subject to the express terms and conditions set forth in **Schedule 31** *(Limitation on Liability)*.

25.6 Performance Guarantee.

Concurrently with the signing of this Agreement, the Service Provider will provide to the Province a duly executed Performance Guarantee, in the form attached as **Schedule 32** *(Performance Guarantee)*.

25.7 Financial Guarantee.

Concurrently with the signing of this Agreement, the Service Provider will deliver to the Province a duly executed Financial Guarantee, in the form attached to this Agreement as **Schedule 33** *(Financial Guarantee)*.

ARTICLE 26 – INSURANCE

26.1 Insurance.

The Service Provider will procure and maintain at all times during the Term of this Agreement, at its own expense and without reimbursement from the Province, the insurance policies more particularly described in **Schedule 34** *(Insurance)*, which will be underwritten by insurers licensed to carry on insurance business in Canada.

26.2 Certificate of Insurance.

The Service Provider will not cancel any of the required insurance policies set out or contemplated in **Schedule 34** *(Insurance)* without thirty (30) days prior written notice to the Province, and consent of the Province where a cancelled insurance policy is not replaced with a replacement insurance policy of the same kind and type, and in an equal or greater amount. Each insurance policy for the above- described insurance coverage will be endorsed to provide the Province with thirty (30) days prior written notice of cancellation or material change. The Service Provider will provide the Province with reasonable evidence of the obtaining of all insurance required to be obtained by the Service Provider, before commencing any Services under this Agreement. Such evidence will be in the Province's form of insurance certificate, as the same may be amended from time to time by the Province and notified by the province to the Service Provider, a copy of which is attached as **Schedule 35** *(Form of Insurance Certificate)*, unless otherwise agreed to in writing by the Province. The Service Provider will provide similar evidence of the continued existence of all required insurance coverage on an annual basis within thirty days of the renewal of such insurance policies, and upon the request of the Province from time to time.

26.3 Adequacy of Insurance.

The Service Provider acknowledges that any requirement or advice by the Province as to the amount of coverage under any policy of insurance does not, and will not be deemed to, constitute a representation by the Province that the amount required under such insurance is adequate, and the Service Provider acknowledges and agrees that it is solely responsible for obtaining and maintaining its own policies of insurance in such amounts as the Service Provider will determine to be appropriate and adequate, subject to the minimum requirements set out on **Schedule 34** *(Insurance)*.

ARTICLE 27 – DISPUTE RESOLUTION

27.1 Informal Dispute Resolution.

In the event of any Dispute, the Parties will use reasonable efforts to settle such Dispute internally and will consult and negotiate with each other in good faith in an effort to reach a fair and equitable solution satisfactory to the Parties. Prior to the initiation of formal dispute resolution procedures, the Parties will

first attempt to informally resolve any dispute, controversy or Claim (including any failure by the Parties to reach agreement where expressly provided for in this Agreement) arising under or in connection with this Agreement as follows:

(a) the Service Provider **[insert relationship manager title]** and the Province **[insert relationship manager title]** will attempt to resolve the Dispute informally by meeting as often, for a duration and as promptly as those representatives deem necessary, to discuss the Dispute and negotiate in good faith in an attempt to resolve the Dispute;

(b) if such persons are unable to resolve the Dispute within a reasonable period, then either one of them may refer the Dispute to the Joint Executive Committee, and the Joint Executive Committee will promptly schedule a meeting to discuss the Dispute and negotiate in good faith in an attempt to resolve the Dispute;

(c) the Joint Executive Committee will meet as often and as promptly as the Parties deem necessary to discuss the Dispute and negotiate in good faith in an effort to resolve the Dispute;

(d) during the course of all discussions referred to in paragraphs (a) to (c) above, all reasonable requests made by one Party to another for non-privileged information, reasonably related to the Dispute, will be provided by the other Party so that both Parties may be fully apprised of the other's interests in the Dispute and resulting positions and interests. The specific format for such discussions will be decided by mutual agreement of the Parties, but may include the preparation of agreed-upon statements of fact or written statements of position or interest;

(e) if the Joint Executive Committee does not resolve the Dispute within (10) Business Days of the referral of the Dispute to the Joint Executive Committee (or such longer period to which the Parties may agree), then either Party may upon written notice to the other Party (the "**Mediation Notice**") elect to submit the Dispute to non-binding mediation, and if such Mediation Notice is accepted in writing within five (5) Business Days of receipt thereof, then the Parties will proceed to mediation in accordance with paragraph (f) below. For greater clarification, either Party may elect to bypass mediation, in which case, the Dispute will be settled by binding arbitration in accordance with Section 27.2 (*Arbitration*);

(f) if the Dispute is referred to non-binding mediation in accordance with paragraph (e) above, then the Parties will thereafter attempt to promptly agree upon and appoint a sole mediator. If the Parties are unable to agree upon a mediator within five (5) Business Days after the effective date of the Mediation Notice (or such longer period as the Parties may agree), then the Parties will bypass mediation and proceed to arbitration in accordance with Section 27.2 (*Arbitration*);

(g) if the Parties agree upon a mediator within the time required pursuant to paragraph (f) above, then the mediation will be conducted at a time, in a city in British Columbia and at a specific location as may be agreed to by the Parties with the mediator, or if the Parties cannot agree, as so designated by the mediator. The mediation will be held within five (5) Business Days after the mediator is appointed. If any Party has substantial need for information from another Party in order to prepare for the mediation, then the Parties will use reasonable efforts to agree on procedures for the formal exchange of information. Each Party will be represented in the mediation by at least an individual with authority to settle the Dispute on behalf of that Party and, if desired by that Party, by legal counsel for

that Party. The Parties' representatives in the mediation will continue with the mediation as long as the mediator reasonably requests, but in no event longer than thirty (30) days from the first day that the Parties meet to commence mediation. Unless otherwise agreed to in writing by the Parties, each Party will pay one-half of the mediator's fees and expenses and will bear all of its own expenses in connection with the mediation. No Party may employ or use the mediator as a witness, consultant, expert, counsel or other similar position regarding the Dispute or any related matters; and

(h) if the parties are unable to resolve the Dispute by mediation, or if either Party elects to bypass mediation entirely, then the matter will be referred to binding arbitration in accordance with Section 27.2 (*Arbitration*).

27.2 Arbitration.

Subject to the provisions of **Schedule 30** *(Indemnification Matters)*, **Schedule 31** *(Limitation on Liability)*, and Section 27.3 (*Special Arbitration*), any Dispute that is not settled in accordance with Section 27.1 (*Informal Dispute Resolution*), will be settled at the request of either Party by binding arbitration in Victoria, British Columbia in accordance with the *Commercial Arbitration Act* (British Columbia) on the following terms:

(a) all hearings will be in held and kept confidence;

(b) the arbitration will be heard before one arbitrator, and if the Parties cannot agree upon an arbitrator within five (5) Business Days of a request from one Party to the other to do so, then each Party will select an arbitrator, and those two arbitrators will jointly select a third arbitrator;

(c) all arbitrators will either be:

(i) a lawyer in good standing with the Law Society or equivalent body in all jurisdictions in Canada where that lawyer is called to the bar,

(ii) a retired lawyer who was previously in good standing with the Law Society or equivalent body in all jurisdictions in Canada where that lawyer was previously called to the bar before that lawyer's retirement; or

(iii) a retired judge;

(d) no individual may be appointed as an arbitrator if that individual is (but for the appointment as arbitrator in connection with a Dispute under this Agreement) or was directly involved in matters relating to this Agreement, the Dispute or the Services to be performed by the Service Provider under this Agreement;

(e) all arbitrators selected or otherwise appointed to hear a Dispute will have experience in complex, commercial outsourcing engagements and be skilled or knowledgeable in the subject matter of the Dispute;

(f) if the arbitration is heard before a panel of three arbitrators, then the decision of the arbitration panel will be made by a majority vote;

(g) judgment upon the award rendered in any such arbitration may be entered in any court having competent jurisdiction;

(h) the Parties will direct the arbitrator (or arbitrators) to make an award of costs, which award will include the remuneration and expenses and any related administrative fees that are charged by the arbitrator (or arbitrators) in connection with the arbitration of the Dispute, as well as the costs and expenses incurred by each Party in preparing for and participating in the arbitration (including the costs related to retaining legal counsel), and the Parties will pay all such costs in accordance with the direction of the arbitrator (or arbitrators);

(i) the Parties will instruct the arbitrator (or arbitrators) to make the final award with respect to the Dispute within 60 days after the hearings have been closed, or such other reasonable period of time (not to be less than thirty (30) days), as may be agreed to in writing by the Parties before the commencement of the arbitration hearings and so notified in writing to the arbitrator (or arbitrators);

(j) notwithstanding anything to the contrary in the *Commercial Arbitration Act* (British Columbia):

(i) the same procedural requirements and rights of discovery as are available under the British Columbia Rules of Court will apply, *mutatis mutandis*, except that the arbitrator (or arbitrators) may make adjustments to the time limits contained in such Rules of Court,

(ii) the laws and rules of evidence applicable in the Courts of British Columbia will apply, and the arbitrator (or arbitrators) may only require the production of relevant documentary and testimonial evidence not protected by the solicitor-client privilege, and

(iii) the arbitrator (or arbitrators) will adjudicate the Dispute by reference to law in accordance with Section 23 of the *Commercial Arbitration Act* (British Columbia), including the precedent of other Court decisions, statutory laws, and laws of interpretation, as would be followed by a Court having competent jurisdiction, and the Parties expressly agree that the Dispute will not be decided upon the law of equity or some other similar basis;

(k) the arbitrator (or arbitrators) will have no power or authority to grant any award or permit any other recourse that would be precluded by the terms of this Agreement, and nor will the arbitrator (or arbitrators) have the power to make any award that addresses matters outside the scope of the Dispute; and

(l) the Parties will be bound by any award issued by the arbitrator (or arbitrators), which award the Parties agree to be bound by and to accept as a final and binding award.

27.3 Special Arbitration.

Any Disputes between the Parties pursuant to Section 6.4 (*Disputes Regarding the Transformation Plan*) will follow the step-by-step resolution procedures set forth in Section 27.1 (*Informal Dispute Resolution*) and to the extent applicable, Section 27.2 (*Arbitration*), provided that the following provisions will apply in respect of any arbitration:

(a) for purposes of Subsection 27.2(i) (*Arbitration*), the arbitrator (or arbitrators) will be instructed to make an award by selecting the submission of one Party over the other, which selected submission will constitute the award of the arbitrator (or arbitrators),

provided that any award of costs contained in such submission may be removed by the arbitrator (or arbitrators) and replaced with an award of costs determined by the arbitrator (or arbitrators) in accordance with the provisions of Subsection 27.2(h) (*Arbitration*);

(b) if any submission includes matters that are outside the scope of the Dispute contemplated in Section 6.4 (*Disputes Regarding the Transformation Plan*), then the arbitrator (or arbitrators) will discard the submission in its entirety as not being in compliance with the scope of the Dispute, and select the other submission for purposes of paragraph (a) above, and if both submission are discounted in their entirety as a result of the application of the provisions of this paragraph, then the arbitrator (or arbitrators) will instruct the Parties, in writing, to resubmit new submissions without such provisions which are outside the scope of the Dispute; and

(c) for greater clarification, the arbitrator (or arbitrators) will not have any jurisdiction, power or authority to grant an award other than as provided for in this Section 27.3 (*Special Arbitration*).

27.4 Confidentiality.

The proceedings of all negotiations, mediations and arbitrations as part of the Dispute Resolution Process will at all times be privately conducted. The Parties agree that all statements and other communications made during the Dispute Resolution Process including, without limitation, offers of settlement, settlement terms and all documents or other materials created for the purposes of the Dispute Resolution Process:

(a) are made on a without prejudice basis;

(b) do not constitute an admission or waiver of rights; and

(c) will not be offered into evidence, disclosed or used for any other purpose other than the Dispute Resolution Process.

During the Dispute Resolution Process, no Party is required to disclose to the other Party any information, documents or materials with respect to which they claim privilege; however, if as part of the Dispute Resolution Process a Party should disclose to the other Party information, documents or materials with respect to which they claim privilege or any information, documents or materials which they regard and identify as confidential or proprietary, then the other Party will maintain the confidentiality of the information, documents or materials so obtained and, to the extent permitted by law, any such disclosure will not constitute a waiver of any privilege or confidentiality. The Parties agree that any information regarding the Dispute Resolution Process, including any decisions or awards made, will not be disclosed to any third parties or used for any purpose other than the Dispute Resolution Process, unless the Parties otherwise agree; provided that nothing in this provision will prevent such disclosure as may be necessary to enforce any arbitration awards.

27.5 Exceptions to Dispute Resolution Procedure.

The provisions of this Article 27 (*Dispute Resolution*) will not be construed to prevent a Party from:

(a) seeking a temporary restraining order or injunctive or other equitable relief with respect to a breach (or attempted breach) of this Agreement by the other Party, to the extent such remedies are available to a Party pursuant to Applicable Law (including, without limitation, the *Crown Proceeding Act* (British Columbia)); or

(b) instituting litigation or other formal proceedings to the extent necessary and available pursuant to Applicable Law:

(i) to enforce arbitration awards or orders for injunctive or other similar relief,

(ii) to avoid the expiration of any applicable limitations period, or

(iii) to preserve a position with respect to other creditors.

27.6 Continuity of Services.

The Service Provider acknowledges that the timely and complete performance of its obligations pursuant to this Agreement is critical to the business and operations of the Province and the continuity of the Services. Accordingly, in the event of a Dispute, and at all times before, during and after the Dispute Resolution Process:

(a) the Service Provider will continue to so perform its obligations and to deliver the Services under this Agreement in good faith during the resolution of such Dispute; and

(b) the Province will continue to pay all Fees payable to the Service Provider in accordance with the terms of this Agreement, other than those Fees which are in Dispute and withheld from payment in accordance with the provisions of Section 15.6 (*Disputed Payments*).

ARTICLE 28 – DEFAULT AND TERMINATION

28.1 Service Provider Material Breach.

The Service Provider will be in material breach of its obligations under this Agreement upon the occurrence of any one or more of the following events or the events set forth in **Schedule 36** *(Material Breach)* (each a "**Material Breach**"):

(a) an Event of Insolvency in respect of the Service Provider, the Performance Guarantor or the Financial Guarantor;

(b) if the Service Provider, the Performance Guarantor or the Financial Guarantor ceases or threatens to cease to carry on business;

(c) any direct or indirect assignment of this Agreement by the Service Provider contrary to the provisions of Section 31.2 (*Assignment by the Service Provider*);

(d) there is, without the Approval of the Province, a corporate or other similar structural reorganization of the Service Provider, the Performance Guarantor or the Financial Guarantor, except for those corporate or other similar structural reorganizations that:

(i) do not result in a direct or indirect assignment of this Agreement by the Service Provider contrary to the provisions of Section 31.2 (*Assignment by the Service Provider*),

(ii) do not adversely affect the Performance Guarantee or the Financial Guarantee in any way, or the ability of the Performance Guarantor or the Financial Guarantor to perform their respective obligations under the Performance Guarantee or the

Financial Guarantee respectively (including, in the case of the Performance Guarantor, to comply with the provisions of the Privacy Obligations), and

(iii) there is no increased risk of a breach of, or an actual breach of, the Privacy Obligations, as determined by the Province in its sole discretion;

(e) any disclosure of Personal Information pursuant to a Disclosure Order, where any director, officer or Manager of the Service Provider or its Subcontractors (or any other Person having similar authority to the foregoing) authorizes, permits or acquiesces in the disclosure of Personal Information pursuant to a Disclosure Order;

(f) any storing, allowing access to, disclosure or use of Personal Information contrary to the provisions of *Freedom of Information and Protection of Privacy Act* (British Columbia) (without the prior written Approval of the Province as may be permitted under *Freedom of Information and Protection of Privacy Act* (British Columbia)); provided that, before the Province requires, in its sole discretion, that the occurrence thereof constitutes a "Material Breach" under this paragraph (f), the Province will have regard to all of the surrounding circumstances including, without limitation, the nature and significance of the breach, the compliance by the Service Provider and its Subcontractors (to the extent applicable) with the Province Policies and the Privacy Obligations, whether such breach is an isolated occurrence and the bearing thereof on the significance of the breach, and the steps and actions taken by the Service Provider (and its Subcontractors, to the extent applicable) to remedy or otherwise deal with the breach (including taking appropriate action against the Person or Persons involved) and the effectiveness and timeliness of such steps and actions so taken, and whether or not the Personal Information in questions has been successfully recovered and whether it was used in any unauthorized way prior to such recovery (it being understood that such consideration will in no way prevent or prohibit the Province from determining that such breach constitutes a "Material Breach");

(g) failing to report the disclosure of Personal Information that is referred to under paragraph (f) above to the Province, provided that the Service Provider will not have committed a Material Breach of this Agreement pursuant to this paragraph (g) until such time as an individual who is a director, officer, Manager or in a Key Position is aware, or ought to have been aware, of such unauthorized access, disclosure or use of Personal Information, and has been provided with reasonable opportunity to report such unauthorized access, disclosure or use to the Province;

(h) taking action against an employee contrary to the provisions of **Schedule 24** *(Privacy Obligations)* which affords whistleblower protection to employees, provided that:

(i) where the Service Provider disputes that it has taken action against an employee contrary to **Schedule 24** *(Privacy Obligations)*, the Service Provider will not have committed a Material Breach of this Agreement as a result thereof until such matter is determined as between the Service Provider and the employee by an agreement in writing, or as a result of an arbitration or court proceeding, as the case may be, where all appeals with respect thereto have been exhausted, or the time to file an appeal has expired without a notice of appeal having been filed, as the case may be, and provided that the Service Provider is proceeding reasonably with respect to any dispute with such employee, and

(ii) in connection therewith, the Province will have regard to all of the surrounding circumstances leading up to any such actions taken by the Service Provider

against the employee, including any use of the whistleblower protection provisions by such employee in order to prevent any disciplinary actions being taken by the Service Provider against such employee for other reasons;

(i) the occurrence of an Service Level Termination Event;

(j) any theft, fraud or other misappropriation of Province funds by the Service Provider, its Personnel or its Subcontractors or their External Personnel;

(k) any matter that is described in this Agreement as constituting a "Material Breach" for which no cure period is provided, and if a cure period is provided, then upon the failure of the Service Provider to rectify such breach within the applicable cure period therefor, or where such breach is not capable of being rectified within such cure period, then if the Service Provider fails to take or continue to take such steps and actions as may be necessary to rectify such breach, and in either case, to the satisfaction of the Province; or

(l) if the Service Provider breaches or defaults in the performance of any of its other material obligations under this Agreement or under any of the other Transaction Documents (other than a Service Level), which has an adverse effect upon the Province, and the Service Provider fails to rectify such breach within thirty (30) days (or such longer period as may be agreed to by the Province on a case-by-case basis) of its receipt of a written notice from the Province requesting it to do so, where such breach is not capable of being rectified within thirty (30) days (or such longer period as may be agreed to by the Province on a case-by-case basis), the Service Provider fails to take or continue to take such steps and actions as may be necessary to rectify such breach, and in either case, to the satisfaction of the Province.

28.2 Remedies of the Province.

Without the requirement for the Province to resort to the Dispute Resolution Process under Article 27 *(Dispute Resolution)* and without limiting any other rights or remedies that the Province may have at law, in equity, or as otherwise set forth in this Agreement, upon the occurrence of a Material Breach, the Province may invoke any one or more of the remedies set forth in **Schedule 37** *(Remedies for Material Breach)*.

28.3 Material Breach by Province.

The Province will be in material breach of its obligations under this Agreement (a "**Province Material Breach**") if the Province fails to pay when due, subject to Sections 15.5 (*Right of Set-Off*) and 15.6 (*Disputed Payments*), an amount in excess of **$[insert number]** payable by the Province to the Service Provider pursuant to this Agreement that has not been subject to a Dispute (or an agreement between the Parties in settlement of a Dispute, whether through arbitration, mediation or otherwise), and the Province fails to rectify such failure within thirty (30) days of its receipt of a written notice from the Service Provider of such failure, such notice to state in detail the nature and specifics of the failure. The Service Provider may extend such thirty (30) day period, in its sole discretion, for such additional period of time upon written notice of such extension to the Province.

28.4 Remedies of the Service Provider.

Without the requirement for the Service Provider to resort to the dispute resolution process under Article 27 *(Dispute Resolution)* and without limiting any other rights or remedies that the Service Provider may have at law, in equity, or as otherwise set forth in this Agreement, upon the occurrence of Province

Material Breach, the Service Provider may immediately terminate this Agreement by the delivery of a Termination Notice to the Province, in which case the provisions of Section 28.7 (*Termination Fees*) will apply.

28.5 Termination by Province for Convenience.

Notwithstanding any other provision contained in this Agreement, the Province may terminate this Agreement for convenience (for any reason or for no reason) on not less than **[insert number]** months prior written notice to the Service Provider at any time during the Term. The Termination Date will be the Termination Date stated in the notice of termination, which date will occur before the expiry of the foregoing notice periods.

28.6 Termination Notice.

Any Termination Notice from one Party to the other under this Agreement will specify the Termination Date, the grounds of termination (if applicable), the reasonable particulars of the surrounding circumstances giving rise to the grounds of termination, and if the Party providing the Termination Notice is the Province, whether any Termination Services will be required by the Province.

28.7 Termination Fees.

The responsibilities of the Parties for termination fees in connection with the Termination of this Agreement are set out in **Schedule 38** *(Termination Fees)*.

ARTICLE 29 – TERMINATION SERVICES

29.1 Termination Services.

Commencing upon the first to occur of the delivery of a Termination Notice and twelve (12) months before the expiry of the Initial Term (in circumstances where the Agreement is not being renewed under Article 2 (*Agreement Term and Renewal*), or the Renewal Term as the case may be, and ending upon the earlier of the completion of the Termination Services or six (6) months after the Termination Date, as such period may be extended pursuant to Section 29.5 (*Extension of Termination Services*) (the **"Termination Assistance Period"**), the Service Provider will provide the Province with the following services to facilitate the Province's repatriation of the Services or the orderly transition and migration of the Services to Alternative Service Provider, as the case may be, in an orderly, effective and efficient manner, and with minimal disruptions or adverse effect to the delivery of the Services (collectively, the **"Termination Services"**):

(a) if the Province intends to consider the use of an Alternative Service Provider, upon the Province's request, assistance to the Province with respect to its describing the Services that will be the subject of a competitive procurement process, bid specification or similar document in respect of the Services provided that if the Parties do not enter into a Renewal Agreement, or if the Province does not provide the Service Provider with a notice of its intention to renew pursuant to Section 2.5 (*Renewal Notice*), then the Service Provider will provide the Province with the services referred to in this paragraph (a) immediately following a request therefor from the Province, notwithstanding that such request may be given by the Province earlier than the times referred to above in this Section 29.1 (*Termination Services*);

(b) cooperation with and assistance to the Province or the Alterative Service Provider in order to facilitate the transfer of the Services to the Province or the Alternative Service

Provider, as the case may be, in an orderly, effective and efficient manner and without any material interruptions or adverse effects to the Services so transferred;

(c) answers to all reasonable questions from the Province or the Alternative Service Provider regarding the Services;

(d) copies of:

(i) the Documentation in electronic format, hard copy or both, as may be requested by the Province including, without limitation, a current listing and copies of all documented operational processes and procedures relating to the provision of the Services as outlined in the Documentation, and

(ii) detailed lists and descriptions of all Services then being provided (including volumes, Achieved Service Levels, up-to-date process maps, workflow charts, and other available policy and procedure documentation), technical information and technical descriptive documentation, and documentation of current configurations, to the extent not already included in the Documentation;

(e) subject to applicable privacy laws then in effect and to Section 29.7 (*Transfer of Personnel*), a current listing of all Personnel, and Subcontractors who are individual independent contractors (whether retained in their individual capacities or through corporate entities), who are performing the Services (**"Available Personnel"**), a description of their roles and specific responsibilities in relation to the Services, whether such Available Personnel are on leave or are active in performing the Services, and their compensation and benefits entitlements;

(f) assistance with the transfer to the Province or the Alternative Service Provider of the Available Personnel in accordance with Section 29.7 (*Transfer of Personnel*);

(g) assistance with the provision of mutually agreed training for those Persons designated by the Province who will be assuming responsibility for the Services following the Termination Date;

(h) copies of Subcontracts relating to the delivery of the Services (whether or not expired with the Term of this Agreement), and provided that such Subcontract were in use or otherwise in effect within three (3) years preceding the Termination Date;

(i) a general list of third person Software licensed and used by the Service Provider during the ordinary course of performing the Services (the **"Termination Licensed Software"**), and the Service Provider will, on the Termination Date, assign and transfer all rights and obligations of the Service Provider with respect to the Termination Licensed Software to the Province at no additional cost to the Province;

(j) a list of any Province Proprietary Software or Service Provider Software and all Modifications thereto used in providing the Services, and copies of all Software and Modifications thereto which is being licensed to the Province in accordance with Article 19 (*Intellectual Property and Proprietary Rights*), or for which the license is being transferred to, or assumed by, the Province or the Alternative Service Provider, and all Source Code for such Software and Modifications for which the Service Provider has access, custody or control;

(k) detailed descriptions of the Systems used in the delivery of the Services sufficient to permit the Province or the Alternative Service Provider to assume control of the provision of the Services or to obtain and implement functional replacements therefor;

(l) assistance with appropriate testing of the Province's transition and migration procedures;

(m) assistance with respect to the transfer of relevant assets to the Province or the Alternative Service Provider in accordance with Section 29.6 (*Transfer of Assets, Contracts and Software*);

(n) the performance of the Service Provider's obligations under the Termination Assistance Plan;

(o) otherwise provide assistance and information requested by the Province in order to enable the smooth transition of the management of the applicable Services from the Service Provider to the Province or the Alternative Service Provider; and

(p) those matters referred to in Section 29.2 (*Termination Assistance Plan*), Section 29.6 (*Transfer of Assets, Contracts and Software*), Section 29.7 (*Transfer of Personnel*), and Section 29.10 (*Additional Termination Arrangements*).

The specific Termination Services to be provided by the Service Provider, including the Termination Services in respect of the foregoing, will be described more fully in the Termination Assistance Plan.

29.2 Termination Assistance Plan.

As part of the Termination Services, the Service Provider will develop and deliver a mutually agreed to termination assistance plan for the transition of the Services from the Service Provider to the Province or to the Alternative Service Provider, as the case may be, in the manner set forth in this Article 29 (*Termination Services*) (the "**Termination Assistance Plan**"). For purposes thereof, the Service Provider will develop the framework for the Termination Assistance Plan within the first **[insert number of months]** months following the Hand-Over Date. The framework for the Termination Assistance Plan will be reviewed by the Parties through the Governance Process on an annual basis. As part of the Termination Services, immediately upon the commencement of the Termination Assistance Period, the Service Provider will, in consultation with the Province and such other persons as the Province may direct, commence in good faith and with all reasonable diligence to develop the complete Termination Assistance Plan based upon the framework described above, and setting out in detail the specific tasks to be accomplished by each Party, and a schedule pursuant to which the tasks are to be completed. Such Termination Assistance Plan will, at a minimum, provide for the following:

(a) a communications plan for Personnel, Subcontractors and other interested parties;

(b) a plan relating to the making of offers of employment to the Available Personnel and the transitioning of employees who accept such offers of employment, and all related employee benefit arrangements in accordance with Section 29.7 (*Transfer of Personnel*);

(c) details of the reversion or transfer of the applicable Systems, the Personal Information, the Province Records, other Province Confidential Information, Province Proprietary Software and other materials and information to which the Province is entitled upon the termination or the expiry of this Agreement;

(d) a plan for the transfer of in-complete IM/IT projects, if any;

(e) a plan for the transfer of tangible personal property and the transfer or assignment of applicable contracts;

(f) support for Systems and Software testing to be carried out by the Province or the Alternative Service Provider in connection with the transfer or licensing of any Systems and Software;

(g) employee training;

(h) any modifications to the Services to be provided during the Termination Assistance Period and the date or dates on which responsibility for the provision of the Services or portions thereof are to be transferred to the Province or the Alternative Service Provider;

(i) any modifications to the Fees to take into account the planned reduction in Services and any increased or decreased costs associated with providing reduced Services over time that are agreed to in accordance with Section 29.3 *(Quality of Services)*;

(j) processes, methods and timelines in respect of the delivery of the Termination Services; and

(k) the anticipated conclusion date for the completion of the Termination Services;

The Parties will monitor the performance of the Termination Services and the Termination Assistance Plan on a regular basis through the Governance Process. The Parties agree to provide to each other reasonably sufficient information to create or update the Termination Assistance Plan as required in accordance with the terms of this Agreement. The Parties will revise and update the Termination Assistance Plan from time to time during the Termination Assistance Period.

29.3 Quality of Services.

The quality and level of performance of the Services by the Service Provider during the Termination Assistance Period will meet the applicable Service Levels then in effect. The Service Provider will not be required to meet the Service Levels with respect to any Services provided during that part of the Termination Assistance Period that occurs after Termination, except as may otherwise be agreed between the Parties through the Governance Process in the completion of the Termination Assistance Plan. The Service Provider will continue to provide the Services during the Termination Assistance Period unless the Province expressly requests the permanent or temporary discontinuation thereof (or a portion thereof). Any permanent or temporary discontinuation of the Services or any part thereof will be set out in the Termination Assistance Plan, or otherwise implemented through the Change Order Process.

29.4 Charges for Termination Services.

During the Term, the Service Provider will provide the Termination Services in the ordinary course of its delivery of the Services at no additional cost or charge to the Province, using all available Personnel and External Personnel. Any Termination Services delivered during the Term that have a material impact on the delivery and performance of the other Services will be deemed to be a Mandatory Change and will be addressed in the manner set forth in Article 7 (*Change Order Process*). After the Term, all Termination Services will be provided at the Standard Time and Materials Rates or Cost-Only Time and Materials Rates, as applicable, in accordance with a budget jointly prepared by the Parties and forming part of the Transition Assistance Plan and based upon the following:

(a) where the Termination is as a result of the expiry of the Initial Term or the Renewal Term, as the case may be, the Standard Time and Material Rates will apply; and

(b) in all other cases of Termination, the Cost-Only Time and Material Rates will apply.

29.5 Extension of Termination Services.

If the Province is unable to complete the transition of Services to the Province or the Alternative Service Provider, as the case may be, by the end of Termination Assistance Period, then upon not less than thirty (30) days prior written notice to the Service Provider, the Province may elect to extend the Termination Assistance Period for up to **[insert number]** months beyond the then-effective date of the expiry of the Termination Assistance Period.

29.6 Transfer of Assets, Contracts and Software.

Upon Termination of this Agreement for any reason, and in connection with the transfer of the responsibility for the performance of the Services to the Province or the Alternative Service Provider, as the case may be, the following provisions will apply:

(a) the Province or the Alternative Service Provider, as the case may be, will have the right (but not the obligation, unless specifically provided otherwise elsewhere in this Agreement) to purchase, or assume the lease of (as applicable), all Dedicated Assets and Designated Contracts from the Service Provider, and the Service Provider will, if such option is exercised, transfer, sell and assign the same to the Province or the Alternative Service Provider, as applicable, on the following terms:

(i) unless otherwise agreed in writing between the Parties or pursuant to the terms of the final Transition Plan, the effective date of transfer of the Dedicated Assets and Designated Contracts from the Service Provider to the Province or the Alternative Service Provider, as the case may be, will be on the Termination Date,

(ii) the Service Provider will be responsible, at its own cost and expense, for obtaining all necessary consents, approvals, authorizations, notices, requests and acknowledgements necessary to assign, transfer and convey such Designated Assets and Designated Contracts to the Province or the Service Provider hereunder, together with all applicable third party and Service Provider warranties associated therewith,

(iii) the purchase price for the Dedicated Assets owned (and not leased) by the Service Provider will be the fair market values of such assets, which the Parties agree will be an amount equal to the net book value of the Dedicated Assets on the books and records of the Service Provider, recorded in accordance with GAAP,

(iv) the Service Provider will sell such Dedicated Assets to the Province or the Alternative Service Provider on an "as-is" basis, free and clear of all Liens,

(v) notwithstanding the provisions of clause (iv) above, upon the exercise of the option to purchase Dedicated Assets as contemplated under this paragraph (a), and prior to the selection of the Dedicated Assets by the Province or the Alternative Service Provider for transfer hereunder, the Service Provider will

provide the Province with a written notice setting forth which, if any, of the Dedicated Assets are not in good working order, normal wear and tear excepted, or are not eligible (where applicable) for maintenance and support services without payment of additional fees or expenses other than ordinary ongoing maintenance and support charges,

(vi) in the case of Dedicated Assets leased by the Service Provider for which the Province or the Alternative Service Provider wishes to acquire the lease, the Service Provider will assign the lease of such Dedicated Assets to the Province or the Alternative Service Provider, on an "as-is" basis free and clear of all Liens other than the interest of the lessor thereof, or such Liens as may have been granted therein by the lessor, and

(vii) any and all transfer and title fees, Taxes and charges in connection with the transfer of the Dedicated Assets under this Section will be borne by the Province;

(b) in respect of any Termination Licensed Software that is being used by the Service Provider to provide the Services (other than off-the-shelf shrink wrap or clip wrap Software), at the option of the Province or the Alternative Service Provider, the Service Provider will transfer or assign the license for such Termination Licensed Software to the Province or the Alterative Service Provider, as the case may be, at no additional cost (other than the requirement for the Province or the Alternative Service Provider to pay ongoing license and maintenance fees, if applicable, in respect of such license);

(c) at the time that the Service Provider licenses any Termination Licensed Software (for use on a dedicated basis for use in providing the Services ((other than off-the-shelf shrink wrap or click wrap Software), the Service Provider will use reasonable efforts to obtain the right to transfer or assign the license upon Termination to the Province or the Alternative Service Provider in accordance with the provisions of paragraph (b) above at no additional charge to be paid to the licensor;

(d) to facilitate the Province's or the Alternative Service Provider's acquisition of the Dedicated Assets, Designated Contracts and Termination Licensed Software, the Service Provider agrees (where commercially practical and subject to express provisions otherwise set forth in this Agreement) to acquire any material assets, Software and other rights in a manner that will enable the Service Provider to transfer the same to the Province or the Alternative Service Provider without the need to obtain and further consents upon the Termination of the Agreement. In the event that the Service Provider is not able to obtain such rights of transfer without having to obtain any further consents at the time of acquisition of any material assets, Software or rights, then the Service Provider will give the Province notice of the same prior to making such acquisition.

29.7 Transfer of Personnel.

Upon the Termination of this Agreement, and subject to Applicable Laws, the Province and the Alternative Service Provider will have the right to extend offers of employment to Available Personnel on such reasonable terms and conditions as the Province or the Alternative Service Provider, as the case may be, may determine. The Service Provider will provide access to such Available Personnel and will not interfere with the recruitment efforts of the Province or the Alternative Service Provider in respect of the Available Personnel.

29.8 Service Provider Severance Costs.

Except as expressly provided in Section 29.9 (*Province Severance Costs*), the Service Provider will be solely liable for any severance, termination or other payments which the Service Provider or an Affiliate of the Service Provider makes, or is required to make, to any of its employees or contractors who do or do not accept the offer of employment made by the Province or the Alternative Service Provider in accordance with Section 29.7 (*Transfer of Personnel*), or who do or do not receive an offer of employment from the Province or the Alternative Service Provider, as the case may be, upon Termination of this Agreement for any reason.

29.9 Province Severance Costs.

With respect to any non-executive Available Personnel of the Service Provider as of the Termination Date, and who do not receive offers of employment from the Province or the Alternative Service Provider (the "**Retained Employees**"), the Service Provider will have the right to seek reimbursement from the Province of the Severance Amount actually paid to any such Retained Employees in respect of the termination of their employment on a without cause basis, provided that:

(a) the Retained Employees are terminated on a without cause basis in connection with the Termination within thirty (30) days of the Termination Date;

(b) the Service Provider gives written notice to the Province requesting reimbursement not less than fifteen (15) days in advance of the intended date of termination of such Retained Employees, such notice to include the name of the Retained Employees whose employment will be terminated by the Service Provider, the proposed Severance Amount, the position and responsibilities of the Retained Employees, and the number of years of employment with the Service Provider (including any continued employment previously with the Province or its prior subcontractor);

(c) the Severance Amount is reviewed and Approved by the Province, acting reasonably and having regard to the requirements of any collective agreement governing the employment of such Retained Employees and Applicable Law;

(d) the Service Provider terminates the employment of such Retained Employees and pays the approved Severance Amount to such terminated Retained Employees within sixty (60) days of the Termination Date;

(e) the Service Provider provides evidence, as may be required by the Province, as to the termination of such Retained Employees and the payment of the approved Severance Amount to such terminated Retained Employees;

(f) to the extent that the Service Provider is entitled to require a release in connection with the payment of the Severance Amount, the Service Provider provides to the Province an originally signed release from such terminated Retained Employees releasing any and all liabilities and obligations of the Province to such terminated Retained Employees; and

(g) with respect to any Retained Employees who are providing the Termination Services to the Province under this Agreement, the dates set forth above in this Section 29.9 (*Province Severance Costs*) will be calculated from and after the last date on which the Termination Services are so provided by such Retained Employees to the Province hereunder, instead of from the Termination Date.

If the Province does not agree with or Approve the proposed Severance Amounts, then the Province will forthwith notify the Service Provider and the Service Provider will then consult with the Province and propose an alternate Severance Amount acceptable to the Province, acting reasonably. If the Parties are unable to agree upon the Severance Amount as between themselves for purposes of reimbursement under this Section 29.9 (*Province Severance Costs*), and regardless of any amount actually paid by the Service Provider to the terminated Retained Employees, then the matter will be a Dispute to be settled in accordance with the Dispute Resolution Process, and the provisions of Article 27 (*Dispute Resolution*) will survive the termination of this Agreement for purposes thereof. The Province will pay the Service Provider the Approved Severance Amount for the terminated Retained Employees pursuant to this Section 29.9 (*Province Severance Costs*) within thirty (30) days of the above conditions being satisfied, including the settlement of and Disputes pursuant to the Dispute Resolution Process.

29.10 Additional Termination Arrangements.

Without limiting the provisions of this Article 29 (*Termination Services*), if this Agreement is Terminated for any reason, then the Service Provider will, effective on the completion of the Termination Services or such other date as may be agreed to between the Parties or as otherwise contemplated in this Article 29 (*Termination Services*):

(a) peacefully leave and cause its Personnel and External Personnel to peacefully leave any Province facilities made available to the Service Provider in connection with providing the Services under this Agreement, and return to the Province and cause its Personnel and External Personnel to return all keys and access cards to such applicable facilities; and

(b) deliver to the Province all Documentation and other files, records and documents relating to the Services and all Province Confidential Information in whatever format, form, condition or media which are then in the possession or control of the Service Provider, or, at the request of the Province, destroy any Province Confidential Information and provide the Province with confirmation of the same.

29.11 Equitable Remedies of the Province.

The Service Provider acknowledges that the Province would suffer irreparable harm if the Service Provider breached (or attempted or threatened to breach) its obligations to provide Termination Services to the Province in accordance with and pursuant to the terms of this Agreement. In such event, the Province may proceed directly to a court of competent jurisdiction without having to exhaust or utilize the Dispute Resolution Process set forth in Article 27 (*Dispute Resolution*). If such court should find that the Service Provider has breached (or attempted or threatened to breach) any such obligations, then the Service Provider will not, without any additional findings of irreparable injury, harm or other conditions to injunctive relief, oppose the entry of an appropriate order compelling performance by the Service Provider and restraining the Service Provider from any further breaches (or attempted or threatened breaches) of its obligation to provide Termination Services hereunder.

29.12 Other Liabilities.

For greater clarification, in no event will the Province or the Alternative Service Provider assume or be liable for, and the Service Provider hereby agrees to indemnify the Province and any Alternative Service Provider from and against, any liabilities or obligations of the Service Provider not expressly assumed under this Agreement or in any other written agreement signed by the Province or the Alternative Service Provider, as the case may be.

ARTICLE 30 – FORCE MAJEURE AND LABOUR DISRUPTION

30.1 Notice of Force Majeure Event.

If either Party is prevented from, or delayed in performing any of its obligations under this Agreement as a result of a Force Majeure Event, or in anticipation of the occurrence of a Force Majeure Event, then the Party claiming the Force Majeure Event (or anticipation of the Force Majeure Event) will promptly notify the other Party by telephone (which does not include, for greater clarification, leaving a voice mail message). That Party will also provide the other Party with a follow up written notice within two (2) Business Days of such Party becoming aware of the potential non-performance or delay, of the particulars of the Force Majeure Event (or anticipation of the Force Majeure Event) including details of the nature of the event, its expected duration and the obligations under the Agreement that will be affected by the Force Majeure Event (or anticipation of the Force Majeure Event). The Party claiming the Force Majeure Event (or anticipation of the Force Majeure Event) will continue to furnish reasonable reports with respect thereto to the other Party on a timely basis during the continuance of the Force Majeure Event. The notice requirements of this Section are in addition to any notices that may be required pursuant to Article 17 (*Business Continuity*).

30.2 Mitigation of Force Majeure Event.

Where a Party becomes aware of the occurrence of an event, condition or circumstance that could reasonably be expected to cause such Party to claim a Force Majeure Event, then that Party will use reasonable efforts to prevent or avoid such event, condition or circumstance developing into a Force Majeure Event, to the extent possible. Failing prevention of the occurrence of such Force Majeure Event by the use of such efforts, the Party claiming the Force Majeure Event will, during the continuance of such Force Majeure Event, use reasonable efforts to mitigate and minimize the effect of such Force Majeure Event, to reduce and minimize any ensuing delay or interruption in the performance of its obligations under this Agreement, and to recommence performance of its obligations under this Agreement whenever and to whatever extent possible and without delay. For greater clarification, where a Force Majeure Event affects performance of the obligations of both Parties under this Agreement, then both Parties may claim the same Force Majeure Event for purposes of this Article 30 (*Force Majeure and Labour Disruption*). Notwithstanding the foregoing, upon the occurrence or expected occurrence of a Force Majeure Event, the Service Provider will forthwith implement the Business Continuity Plan.

30.3 Application of Business Continuity Plan.

Upon the occurrence or expected occurrence of a Force Majeure Event, if:

(a) the Service Provider forthwith implements the Business Continuity Plan as contemplated in accordance with the terms thereof; and

(b) provided that the Business Continuity Plan complies with the requirements of, and the Service Provider has performed all of its obligations under, Article 17 (*Business Continuity*);

then to the extent that the Business Continuity Plan does not contemplate the particular Force Majeure Event in question or otherwise provide remedies that adequately address the same, the provisions of Section 30.4 (*Consequences of Force Majeure Event*) will apply.

30.4 Consequences of Force Majeure Event.

Subject to the provisions of Section 30.3 (*Application of Business Continuity Plan*), during the occurrence of a Force Majeure Event, the obligations of the Party claiming the Force Majeure Event will be suspended, but only to the extent that such Party's obligations cannot be performed or are delayed as a result of the Force Majeure Event, and such Party will not be considered to be in breach or default under this Agreement for the period of such occurrence. The suspension of performance will be no greater in scope and of no longer duration than is reasonably required to adjust for effects of the Force Majeure Event, to the extent reasonably possible to do so. For greater clarification, no obligation of either Party that existed prior to the Force Majeure Event causing the suspension of performance will be excused as a result of the Force Majeure Event, unless such obligation is a continuing obligation, the performance of which is affected by the Force Majeure Event. During any Force Majeure Event, the Province may, in its discretion, exercise any one or more of the following remedies:

(a) during the period of time such Force Majeure Event remains in effect, not pay that portion of the Fees in respect of any Services so affected by the Force Majeure Event; and

(b) procure or otherwise obtain alternative services from any Person in replacement for or substitution of the affected Services during the period of time that the Force Majeure Event remains in effect, and for greater clarification, includes right of the Province to use the Fees so withheld from the Service Provider in accordance with paragraph (a) above to pay any such other Person for the alternative services.

30.5 Establishing a Force Majeure Event.

The Party claiming that a Force Majeure Event has occurred will bear the burden of proving the existence of such a Force Majeure Event and the consequences of such event.

30.6 Labour Disruption.

In the event of an occurrence or potential occurrence of a Labour Disruption preventing or delaying the performance of the obligations of the Service Provider under this Agreement, the Service Provider will:

(a) promptly notify Province by telephone of the particulars of the Labour Disruption including details of the nature of the Labour Disruption, its expected duration and the obligations of the Service Provider under this Agreement that will be affected by such Labour Disruption; and

(b) continue to furnish reasonable reports with respect to the status of the Labour Disruption to the Province on a timely basis during the continuance of the Labour Disruption.

In respect of the foregoing notice to the Province, the Service Provider may leave a voicemail message with the Province if necessary, but such voicemail message will not be deemed to be notice until actual voice contact is made, and the Service Provider will follow-up with written notice within three (3) Business Days of any verbal contact. Prior to claiming a Labour Disruption, the Service Provider will use its reasonable efforts to prevent or avoid the Labour Disruption, but not to the extent that the Service Provider would suffer substantial harm to its own commercial interests.

30.7 Effect of Labour Disruption.

A failure to provide any Services as a result of a Labour Disruption will not give rise to a Material Breach under this Agreement provided that the Service Provider continues to perform and provide the disrupted Services as soon as possible and continues to so use such efforts until the affected Services are restored.

30.8 Other Remedies.

During a Labour Disruption, the Province may, in its discretion, exercise any one or more of the following remedies in respect of the Services:

(a) not pay the Fees in respect of such other Services so affected (other than direct additional costs incurred by the Service Provider related to a partial delivery of such Services) during the period of time that the Labour Disruption remains in effect and such Services are disrupted or delayed; and

(b) procure or otherwise obtain alternative services from any Person in replacement for or substitution of the affected Services during the period of time that the Labour Disruption remains in effect and such Services are disrupted or delayed, and to off-set or deduct any costs thereof that are in excess of the Fees withheld pursuant to paragraph (a) above against any other Fees payable to the Service Provider under this Agreement.

30.9 Suspension of Maximum Credit Amount.

During the continuance of a Labour Disruption, the application of the Weightings for determining the Service Level Credits for those Services that are directly affected by the Labour Disruption will be suspended, such that the occurrence of the Labour Disruption will not adversely affect the requirement of the Service Provider to pay the Service Level Credits in respect thereof, unless the Service Provider has failed to comply with this Article 30 (*Force Majeure and Labour Disruption*) including, without limitation, the requirement of the Service Provider to remedy the failure and to perform and provide the Services caused by the Labour Disruption.

ARTICLE 31 – ASSIGNMENT

31.1 Assignment by Province.

The Province may assign at any time, in its sole discretion, and without the Approval of the Service Provider but upon prior written notice, this Agreement in whole or in part, or sublicense any right or benefit set forth in this Agreement to any government, public sector or Crown entity, body or authority. Nothing in this Section will limit, or be deemed to limit, any rights granted in this Agreement with respect to Alternative Service Providers.

31.2 Assignment by Service Provider.

The Service Provider will not, either directly or indirectly, in whole or in part, assign this Agreement or any rights, duties, obligations or interests of the Service Provider under this Agreement, without the prior written consent of the Province, which consent may be given or withheld in the sole and absolute discretion of the Province. For the purpose of this Agreement, the following will be deemed to be an assignment:

(a) the amalgamation of the Service Provider or the Performance Guarantor with any other entity other than amalgamations with other Affiliates of the Service Provider that do not:

(i) cause a change in the Corporate Control of the Service Provider or the Performance Guarantor that would not be permitted under paragraph (d) below,

(ii) result in direct foreign ownership of any kind of the Service Provider or the Performance Guarantor, or

(iii) result in the Service Provider or the Performance Guarantor ceasing to be Canadian Entities;

(b) an assignment by operation of law (but not including assignments by operation of law as a result of amalgamations permitted under paragraph (a) above);

(c) a sale of all or substantially all of the assets or undertaking of the Service Provider, the Performance Guarantor or the Financial Guarantor;

(d) a direct change in the Corporate Control of the Service Provider or the Performance Guarantor, other than a direct change in Corporate Control of the Performance Guarantor in circumstances where:

(i) the Performance Guarantor:

(A) continues to be a Canadian Entity,

(B) is owned only by Canadian Entities such that there is no direct foreign ownership of the Performance Guarantor, and

(C) continues to be under the Corporate Control of an Affiliate of the Financial Guarantor, and

(ii) any such change in Corporate Control does not adversely impact or otherwise adversely affect the Performance Guarantee or the Financial Guarantee, as determined by the Province in its discretion; or

(e) any direct foreign ownership of any kind of the Service Provider or the Performance Guarantor.

Any attempt by the Service Provider to so assign all or any part of this Agreement or any of the Service Provider's rights, duties, obligations or interests under this Agreement, without the prior written consent of the Province, will be null and void and without effect, and will constitute a Material Breach of this Agreement under Subsection 28.1(k) (*Service Provider Material Breach*), giving rise to the right of the Province to terminate this Agreement. For greater clarification, at no time will the Province consent to any assignment where such assignment could in any manner expose any Personal Information to any increased risk of access, use or disclosure contrary to the terms of this Agreement. Notwithstanding the foregoing, the Subcontracting by the Service Provider of any of its rights, duties, obligations or interests under this Agreement in accordance with the provisions of Article 12 (*Subcontractors*) will not constitute or be deemed to constitute an assignment under this Section 31.2 (*Assignment by Service Provider*).

ARTICLE 32 – CONTRACTUAL RELATIONSHIP

32.1 Relationship of the Parties.

Except as otherwise set forth in this Agreement:

(a) nothing in this Agreement will be construed to grant the Service Provider any right to act as an agent for or on behalf of the Province, including with respect to the Stakeholders, the customers of the Services, third parties or any other Person; and

(b) the Service Provider has no authority to bind, and will not bind or purport to bind, the Province with respect to any such Stakeholders, customers, third parties or any other Person with respect to the performance of the Services or any matter relating to the Services, without the express Approval of the Province.

For greater clarification, the use by the Service Provider of the Province Marks in performing the Services under this Agreement, and the assumption by the Service Provider or its Affiliates of any Assigned Contracts, will not be, or be deemed to be, an act of the Service Provider (or its Affiliates, as applicable) as agent for and on behalf of the Province, and in all such cases the Service Provider (or its Affiliates, as applicable) will be, and will be deemed to be, acting on its own behalf, in its own right and as a independent contractor. The Service Provider expressly agrees not to act or to purport to act as agent for and on behalf of the Province, and not to bind or to purport to bind the Province, unless authorized to do so by express and prior Approval of the Province.

32.2 No Partnership or Joint Venture.

This Agreement establishes, and will only be construed as establishing, a contract between unrelated business entities for the provision of certain services, and does not and will not be construed or deemed to create or constitute a partnership or joint venture relationship between the Parties. Each Party hereby expressly disclaims any intention to create a partnership or a joint venture with respect to the subject matter of this Agreement. Each Party will be independently and solely responsible for all obligations arising in connection with its own employees (including any obligations incumbent upon such Party as an employer, such as the payment of benefits, and the withholding and remittance of applicable source deductions, in respect of its employees).

32.3 Conflict of Interest.

At no time during the Term will the Service Provider or its Personnel directly or indirectly engage in any activity, business or undertaking that could create a conflict of interest or perceived conflict of interest with the Province in respect of all or any part of the Services (it being acknowledged by the Parties that the different economic interests of the Parties in and of itself will not be deemed to be a conflict of interest under this Section). In connection therewith, the following provisions will apply:

(a) where the Service Provider becomes aware of any act, omission or event that could be construed as creating a conflict of interest or a perceived conflict of interest in respect of all or any part of the Services, or where the Service Provider is uncertain as to whether or not a conflict of interest or a perceived conflict of interest could exist in a particular situation, the Service Provider will immediately notify the Province of the same;

(b) the Service Provider will abide by any direction given by the Province in respect of any such act, omission or event, except where the Service Provider reasonably disagrees with such direction from the Province, in which case such matter will be deemed to be a Dispute and will be resolved in accordance with the Dispute Resolution Process;

(c) if such Dispute is settled by arbitration, then the Dispute will be determined by the arbitrator (or arbitrators) in accordance with any Province Policies or processes demonstrably utilized or held by the Province in respect of conflicts of interest;

(d) the Province retains the right to prohibit any Person (including any Subcontractor or Supplier to of the Service Provider) from taking any action, delivering any Services or otherwise participating in any manner with respect to the Services or to this Agreement where the Province determines, in its sole opinion, that such Person's current or past corporate or other interests may give rise to a conflict of interest in connection therewith; and

(e) any determination or direction by the Province in respect of paragraph (d) above will be based upon such information as the Province, in its sole discretion, determines to be relevant.

32.4 Code of Conduct and Standards.

The Service Provider will at all times comply, and will cause its Personnel to comply, with the Service Provider code of conduct policy, a copy of which is attached to this Agreement as **Schedule 39** *(Service Provider Code of Conduct)*, as such policy is revised from time to time upon written notice to the Province. The Service Provider will also require its Personnel to conduct themselves in a manner consistent with the "conflicts of interests" guidelines as set forth in the *Standards of Conduct for Public Services Employees* (British Columbia), a copy of which has been provided by the Province to the Service Provider, as such standard is revised by the Province from time to time upon notice to the Service Provider (but excepting out compliance with any such revised standards that could reasonably result in adverse labour relations between the Service Provider and those of its Personnel who are governed by a collective agreement then in force). Should there be a conflict or inconsistency between the Service Provider code of conduct policy and the Province's the *Standards of Conduct for Public Services Employees* (revised from time to time as previously provided), then the higher or more stringent code of conduct, policy or standard will govern.

32.5 Province's Conflict of Interest Policy.

The Service Provider represents, warrants and covenants that none of its members or employees has given, and nor will they give, any commissions, payments, kickbacks, lavish or excessive entertainment, or other inducements of more than minimal value in any form to any employee or agent of the Province in connection with this Agreement. The Service Provider acknowledges that the giving of any such inducements or gifts is strictly in violation of the Province's policy on conflicts of interest, and may result in cancellation of this Agreement and all future contracts between the Parties. The Service Provider acknowledges that it has read the Province's policy on conflicts of interest, and it agrees that it will abide by such policy during the Term, as such policy is revised from time to time upon reasonable notice to the Service Provider.

ARTICLE 33 – MISCELLANEOUS

33.1 Notice.

Unless specifically provided otherwise in this Agreement, including through the Governance Process, wherever any notice, communication, demand, invoice, Approval or other document is required or permitted to be given, sent or delivered by one Party to another under this Agreement, then it will be in writing and may be delivered personally, by facsimile or sent by a recognized courier service (and for greater clarification, no notice, demand or Approval required or permitted to be given under this Agreement will be, or be deemed to be, effective or delivered if given by email). Any such notice, communication, demand, invoice, Approval or other document so personally delivered or sent by facsimile or courier will be deemed to be given when actually received and will be addressed as follows:

To the Province:

The Province of British Columbia
[insert address]
[insert city], British Columbia
[insert postal code]

Attn: **[insert title]**
Fax: (604) **[insert]**
To the Service Provider:

[insert name and address]

Attn: **[insert title]**
Fax: (604) **[insert]**

Either Party may change its address or facsimile number for notices upon giving prior written notice of the change to the other Party in the manner provided above.

33.2 Appropriation and Approvals.

Notwithstanding any other provision of this Agreement, the payment of money by the Province to the Service Provider under this Agreement is subject to:

(a) there being sufficient monies available in an appropriation, as defined in the *Financial Administration Act* (British Columbia), to enable the Province to make that payment; and

(b) Treasury Board, as defined in the *Financial Administration Act* (British Columbia), not having controlled or limited, under the *Financial Administration Act* (British Columbia), expenditure under any appropriation referred to in paragraph (a) above.

33.3 Severability.

If any provision contained in this Agreement or its application to any Person or circumstance will, to any extent, be invalid or unenforceable, then the remainder of this Agreement or the application of such provision to Persons or circumstances other than those to which it is held invalid or unenforceable, will not be affected, and each provision of this Agreement will be separately valid and enforceable to the fullest extent permitted by law. In addition, any provision of this Agreement which is prohibited or unenforceable in any jurisdiction will not invalidate the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction will not invalidate or render unenforceable such provision in any other jurisdiction. In respect of any provision determined to be unenforceable or invalid in a court having competent jurisdiction, the Parties agree to negotiate in good faith to replace the unenforceable or invalid provision with a new provision that is enforceable and valid in order to give effect to the business intent of the original provision to the extent permitted by Applicable Law, and in accordance with the intent of this Agreement. For greater clarification, if the application of any provision of this Agreement, either generally or in a particular situation, would require a Party to act in a manner contrary to Applicable Law, then such provision will be deemed to be stricken from this Agreement (either generally or in such particular situation, as appropriate), and the affected Party will not be in breach of the Agreement or liable for damages for complying with such Applicable Law.

33.4 Entire Agreement.

This Agreement and the Schedules to this Agreement, together with the other Transaction Documents, and all other documents or agreements referred to in this Agreement, the Schedules and the other Transaction Documents, constitute the entire agreement among the Parties with respect to the subject matter hereof, and cancel and supersede any other prior agreements, undertakings, declarations, commitments, representations, warranties, conditions, promises and understandings, whether written or oral, express or implied, statutory or otherwise among the Parties with respect to the subject matter of this Agreement.

33.5 Amendments.

No term or provision of this Agreement may be amended except by written instrument signed by each of the Parties, by a Change Order as contemplated in Article 7 (*Change Order Process*), or by a unilateral notice of declaration given or made by one Party pursuant to the terms of this Agreement, in respect of a change or amendment that such Party is entitled to make under the terms of this Agreement without the requirement for the Approval of the other Party, if any.

33.6 No Liens or Charges against Provincial Assets.

Except as expressly provided in this Agreement, the Service Provider covenants and agrees to protect and keep free of all assets used in the provision of the Services and assets of the Province from any and all Liens, other than interests of a lessor in any leased assets or Liens granted by any lessor in such leased assets. If any such Lien is filed, then the Service Provider will immediately notify the Province by providing a copy of the Lien claim, and will cause such Lien to be satisfied or otherwise discharged within ten (10) Business Days. If any such Lien is filed or otherwise imposed, and the Service Provider does not cause such Lien to be released and discharged forthwith, then the Province has the right, but not the obligation, to pay all sums necessary to obtain such release and discharge, or otherwise cause the Lien to be removed to the satisfaction of the Province, from funds retained from payment then due or thereafter to become due as Fees payable to the Service Provider under this Agreement.

33.7 Waiver.

Failure by a Party to insist in any one or more instances upon the strict performance of any one of the terms, provisions or covenants contained in this Agreement will not be construed as a waiver or relinquishment of such term, provision or covenant. No consent or waiver, express or implied, by a Party to or of any breach or default by another Party in the performance by such other Party of any term, provision or covenant under this Agreement will be deemed or construed to be a consent or waiver to or of any other breach or default such other Party under this Agreement. No waiver of any breach of any term, provision or covenant of this Agreement will be effective or binding unless made in writing and signed by the waiving Party.

33.8 Further Assurances.

Each of the Parties will, from time to time, execute and deliver all such further documents and instruments and do all such further acts and things as the other Party may reasonably require to carry out or better evidence or perfect the full intent and meaning of this Agreement.

33.9 Obligations as Covenants.

Each obligation of a Party in this Agreement, even though not expressed as a covenant, is considered for all purposes to be a covenant.

33.10 Transaction Fees.

Each Party will be responsible for and pay its respective legal and accounting costs and other expenses incurred in connection with the preparation, execution and delivery of this Agreement (including all prior steps and actions taken in respect to the JSRFP), the other Transaction Documents and all other documents and instruments prepared, executed or delivered pursuant thereto or to this Agreement.

33.11 Survival.

Unless otherwise provided in this Agreement, the following provisions, including the obligations of the Service Provider and the Province thereunder will survive the expiration or termination of this Agreement:

- Section 1.4 (*Interpretation*);
- Section 1.5 (*Acting Reasonably*);
- Section 2.10 (*Termination Assistance*);
- Section 2.11 (*Effect of Termination*);
- Section 3.12 (*Effect of Termination Prior to Hand-Over Date*);
- Section 10.1 (*Province Marks*);
- Section 10.4 (*Publicity*);
- Section 12.1 (*Responsibility for Subcontractors*);
- Section 14.1 (*Maintenance of Records*)
- Section 14.3 (*Custody of Province Records*);
- Section 14.4 (*Control of Province Records*)
- Section 14.5 (*Final Return of Province Records*);
- Section 14.7 (*Storage and Disposal of Records*);
- Section 14.8 (*Locations of Records*);
- Section 15.5 (*Right of Set-Off*);
- Section 15.6 (*Disputed Payments*);
- Section 16.2 (*Foreign Discourse*);
- Section 16.6 (*Safeguarding Confidential Information*);
- Section 16.7 (*Permitted Disclosures and Use of Confidential Information*);
- Section 16.8 (*Province Permitted Disclosure*);
- Section 16.9 (*Exceptions to Obligations of Confidentiality*);
- Section 16.10 (*Disclosures Compelled by Law*);
- Section 16.11 (*Disclosure of Personal Information*);
- Section 16.12 (*Court Order Disclosure*);
- Section 16.13 (*Notification of Unauthorized Use of Confidential Information*);

- Section 16.14 (*Breach of Confidentiality*);
- Section 16.15 (*No Rights to Confidential Information*
- Section 19.1 (*Ownership of Other Assets*);
- Section 19.2 (*Ownership of Province Software and Modifications*);
- Section 19.3 (*Assignment by the Service Provider*);
- Section 19.4 (*Personnel, Subcontractors and External Personnel*);
- Section 19.6 (*Province License*);
- Section 19.7 (*Service Provider License to Modifications*);
- Section 19.8 (*Use of Confidential Information in License Rights*);
- Section 20.12 (*Termination of Rights to Province Shared Infrastructure*);
- in respect of an audit conducted by the Province of the last Contract Year, Section 22.1 (*Access Rights*), Section 22.2(*Examination and Copies*), Section 22.4 (*Audit Rights*), Section 22.5 (*Costs*, and Section 22.7 (*General Principles*);
- Section 23.3 (*FOIPPA Inspections*);
- Article 25 (*Indemnification, Liability and Guarantees*);
- Article 27 (*Dispute Resolution*);
- Section 28.7 (*Termination Fees*);
- Article 29 (*Termination Services*);
- Section 31.2 (*Assignment by Service Provider*);
- Section 33.11 (*Survival*);
- **[insert other provisions that should survive, as applicable, including from the Schedules];**
- the Performance Guarantee and the Financial Guarantee; and
- any other provisions of this Agreement which are required for the proper interpretation thereof.

In addition, any liabilities or obligations of either Party arising before Termination of this Agreement or arising out of the events causing such Termination, and any damages or other remedies to which a Party may be entitled under this Agreement, whether at law or in equity, arising from any breach of such obligations of a Party and any other provisions herein, the nature and intent of which is to survive Termination of this Agreement, will survive and will not be affected by the expiration or Termination of this Agreement.

33.12 Language.

The Parties have agreed that this Agreement and all documents related to this Agreement will be drafted in the English language. Les parties aux présentes ont convenu que cette convention et tous les documents qui s'y rapportent soient rédigés en langue anglaise.

33.13 Governing Law.

(a) This Agreement will be governed by and construed in accordance with the laws, other than choice of law rules, of the Province of British Columbia. Any matter regarding the interpretation and application of this Agreement or the other Transaction Documents, and all disputes arising under or in connection with this Agreement or the other Transaction Documents will, subject to Article 27 (*Dispute Resolution*), be within the exclusive jurisdiction of the courts of British Columbia, as stipulated in the following paragraph.

(b) Subject to Article 27 (*Dispute Resolution*), the Parties irrevocably agree to and hereby accept and attorn to the exclusive jurisdiction of the Courts of British Columbia for any and all Claims that they may have related in any way to this Agreement and its renewal or non-renewal, and all Disputes relating hereto or hereunder, and the Parties irrevocably covenant and agree not to commence any action or bring any Claim in any forum whatsoever, be it domestic, foreign or international (including, but not limited to the *North American Free Trade Agreement*), relating in any way to this Agreement or its renewal or non-renewal or any Dispute relating hereto or hereunder.

(c) The Parties further agree that, should any third party initiate any action under any of the dispute settlement provisions of the *World Trade Organization Agreement* or the *North American Free Trade Agreement* (including but not limited to Chapter Eleven thereof), in any way relating to this Agreement, then no Party will provide any assistance whatsoever (including, without limitation, financial assistance, access to documents and access to personnel) to such third party to pursue any such action. The Parties will also provide all reasonable assistance, one to the other, to defend against such third party claims.

(d) The Service Provider, on its own behalf and on behalf of all others who may claim through it or under it, including but not limited to the Performance Guarantor and the Financial Guarantor and their respective Affiliates (collectively, the "**Service Provider Group**") hereby covenants and agrees that, without the express written consent of the Province (which may be withheld for any cause, or without cause), none of the Service Provider Group will make any Claim or take any proceedings whatsoever concerned or related to any matter arising under or relating to this Agreement against any Person under Chapter Eleven of *the North American Free Trade Agreement*.

(e) The Service Provider, on its own behalf and on behalf of the Service Provider Group, hereby specifically acknowledges that the provisions of this Section 33.13 (*Governing Law*) are fundamental to this Agreement. The Province has fundamentally relied upon the presence of all of these provisions and the Province would not have entered into this Agreement with the Service Provider without these provisions being included.

33.14 Change of Law.

The Service Provider hereby acknowledges and agrees that its costs involved in performing its obligations under this Agreement are, in part, based upon governmental laws, regulations and policies in force at the time this Agreement was entered into and subsequently, and that such governmental laws, regulations and policies are subject to change without notice. Any such change could result in a material change in the Service Provider's costs of performing its obligations under this Agreement. The Service Provider specifically acknowledges and agrees that:

(a) any such change that has the effect of increasing the Service Provider's costs of performing its obligations under this Agreement will not effect those obligations;

(b) such actions will not constitute expropriation or be tantamount to expropriation at domestic or international law (including, but not limited, the *North American Free Trade Agreement*); and

(c) such actions will not constitute grounds for asserting any other claim whatsoever under domestic law or any claim whatsoever under any international agreement (including, but not limited to, Chapter Eleven of the *North American Free Trade Agreement* and the *General Agreement on Trade in Services*).

33.15 No Fettering of Legislative Authority.

The Service Provider expressly acknowledges and agrees that nothing in this Agreement will be construed as an agreement by the Province to restrict, limit or otherwise fetter in any manner the Province's ability to introduce, pass, amend, modify, replace, revoke or otherwise exercise any rights or authority regarding legislation, regulations, policies or any other authority of the Province.

33.16 Procurement.

The Parties hereby acknowledge and affirm that this Agreement constitutes a "procurement" by the Province as that term is utilized in the *North American Free Trade Agreement* and the *General Agreement on Trade in Services*, and consequently:

(a) *North American Free Trade Agreement* Articles 1102, 1103, 1107, 1106(1)(b), (c), (f), and (g), and 1106(3)(a) and (b) do not apply to this Agreement, by virtue of the *North American Free Trade Agreement* Articles 1108(7)(a) and 1108(8) (b);

(b) *North American Free Trade Agreement* Chapter Twelve does not apply to this Agreement by virtue of Article 1201(2)(c);

(c) the Services being procured under this Agreement are services supplied in the exercise of governmental authority for purposes of the *General Agreement on Trade in Services*; and

(d) Articles II, XVI and XVII of the *General Agreement on Trade in Services* do not apply to this Agreement because, for purposes of Article XIII of that agreement, this Agreement constitutes a procurement by a governmental agency of services being purchased for governmental purposes and not with a view to commercial resale or with a view to use in the supply of services for commercial sale.

33.17 Binding Effect.

This Agreement will be binding upon and enure to the benefit of the Parties and their respective successors and permitted assigns.

33.18 No Third-Party Beneficiaries.

Nothing in this Agreement, express or implied, is intended to confer upon any Person (other than the Parties and their successors and permitted assigns), and the indemnified parties who are expressly indemnified pursuant to the provisions of this Agreement, any rights, benefits or remedies of any kind or character whatsoever, and no Person will otherwise be deemed to be a third-party beneficiary under or by reason of this Agreement, unless specifically provided otherwise in this Agreement.

33.19 Counterparts.

This Agreement may be executed in several counterparts, each of which will be deemed to be an original. Such counterparts together will constitute one and the same instrument, notwithstanding that all of the Parties are not signatories to the original or the same counterpart.

SCHEDULE 1

DEFINITIONS
(Section 1.1)

"Acceptance Date" has the meaning given to it in Subjection 6.6(e) (*Acceptance Testing*).

"Acceptance Test" means a test in respect of a Stage using the principles and procedures set out in Section 6.6 (*Acceptance Testing*) and in the Transformation Plan, which is to be used by the Province to determine whether the deliverables for such Stage conform with the Transformation Plan and in particular, that the Critical Issues are adequately addressed.

"Access Subcontractor" means a Subcontractor who has, or could have, access to or custody of Personal Information.

"Achieved Service Levels" means, in respect of any Service Level and for any measurement period, the standard and level of performance, as applicable, actually achieved by the Service Provider in respect of the particular Service Level for the measurement period in question.

"Adverse Impact" has the meaning given to it in Section 7.5(g) (*Change Request Process*).

"Affiliate" has the meaning given to it in the *Business Corporations Act* (British Columbia) and in addition, when used in connection with the Service Provider, includes any member of the Service Provider Group.

"Agreement" means this BPS Services Agreement Template, all Schedules attached to this BPS Services Agreement Template and the Transaction Documents, as the same may be changed, modified, amended, supplemented or updated from time to time, including by way of Change Orders, a Renewal Agreement or as otherwise permitted hereunder.

"Alternative Service Provider" means any Person or Persons designated by the Province from time to time as an alternative service provider for any or all of the Services, but only after such Person or Persons have been so designated by the Province as such.

"Annual Operating Plan" has the meaning given to it in Section 13.5 (*Annual Operating Plan*).

"Applicable Laws" means all applicable laws, including any statute, regulation or by-law, treaty, directive, policy having the force of law, order, judgment, injunction, award or decree of any Canadian or Provincial Governmental Authority, in Canada or in any Province in Canada, which is binding on the Parties (or on one Party as applicable), and in effect from time to time or are otherwise applicable to the performance of the Services, but does not include any law, statute, regulation or by-law, treaty, directive, policy having the force of law, order, judgment, injunction, award or decree of a foreign jurisdiction outside of Canada.

"Approval" means, with respect to any matter, document, action or other thing to be consented to or otherwise approved, that the same action has the prior written approval of the Party in question, and **"Approved"** has a similar meaning.

"Assigned Contract" means a contract entered into between the Province and a third party for the delivery and provision of goods and services, or the license of any Software, in connection with or relating to the Services contemplated in this Agreement, and assigned or to be assigned by

the Province to the Service Provider pursuant to the Master Transfer Agreement, as listed in the Master Transfer Agreement, but in respect of each particular "Assigned Contract" only from the date that such assignment to the Service Provider is effective, and only until such time as the Service Provider renews, extends, renegotiates or otherwise amends the terms thereof (unless expressly Approved otherwise by the Province).

"Assigned Subcontractor" means a Subcontractor who is a party to an Assigned Contract.

"Available Personnel" has the meaning given to it in Subsection 29.1(e)(*Termination Services*).

"Basic Infrastructure Credit" has the meaning given to it in Section 20.2 (*Use of Province Shared Infrastructure*).

"Basic Services " has the meaning given to it in Subsection 4.1(b) (*Overview of Services*)

"Benchmarker" has the meaning given to it in Subsection 9.1(c) *(Benchmarking)*.

"Benchmarking" has the meaning given to it in Section 9.1 *(Benchmarking)*.

"Broader Public Sector" means crown corporations or agencies that are owned directly or indirectly by the Province, and all other levels of government within British Columbia including, without limitation, all municipalities, cities, towns, counties or other political jurisdictions of British Columbia, or any agency, board, council, department, authority, tribunal or commission of the Province or of any of the foregoing, and includes any universities, colleges, schools, school boards, hospitals and health authorities in British Columbia.

"Business Continuity Plan" means a roadmap and description of procedures, information and advance arrangements to guide the timely recovery and ongoing provision of services, programs and operations within a predefined period of time, following the declaration of a Disaster or any other similar event that interrupts operations or disrupts the delivery of the Services, including a disaster recovery plan which details the back-up and recovery procedures to be followed by the Service Provider in the event of a Disaster for Systems supporting essential Services.

"Business Day" means any day other than a Saturday, Sunday or a statutory holiday in the Province of British Columbia.

"Canadian Entity" has the meaning given to it in Section 16.4 *(Canadian Entities)*.

"Change Order Process" has the meaning given to it in Section 7.4 (*Change Request*).

"Change Order" has the meaning given to it in Section 7.9 (*Change Orders*).

"Change Request" has the meaning given to it in Section 7.4 (*Change Request*).

"Claims" means any and all claims, legal or other proceedings, suits, actions, causes of action, losses, damages, liabilities, costs and expenses (whether accrued, actual, contingent, latent or otherwise), and all reasonable legal fees suffered or incurred by a Person.

"Communication Plan" means the communications protocols and processes to be followed by the Service Provider in connection with any Communications to the Stakeholders, or to other

Persons, in connection with the Services and this Agreement, as more particularly described in **Schedule 17** *(Communications Plan and Processes)*.

"Compelled Party" has the meaning given to it in Section 16.10 *(Disclosure Compelled by Law)*.

"Confidential Information" means the Province Confidential Information and/or the Service Provider Confidential Information, as the case may be.

"Contaminant" has the meaning given to it in Section 18.5 *(System Contaminants)*.

"Contract Year" means each twelve (12) month period commencing on April 1 of a particular year and ending on March 31 of the immediately following year, except that the following will apply, as applicable:

(a) the first "Contract Year" will be a partial "Contract Year" commencing on the Effective Date and ending on March 31, of the immediately following year; and

(b) the final Contract Year will be a partial "Contract Year" commencing on April 1 in the final year and ending on Termination.

"Control" means the power or authority to manage, restrict, regulate or administer the use or disclosure of a Record.

"Corporate Control" of a corporation or other entity is directly held by a Person where securities of the corporation or other entity to which are attached 50% or more of the votes that may be cast to elect directors or persons acting in a similar capacity of the corporation or other entity are directly held, other than by way of security only, by or for the benefit of such Person, and **"Corporately Controlled"** has corresponding meaning.

"Corporate Structure" has the meaning given to it in Section 16.3 (*Corporate Structure and Corporate Chart*).

"Cost-Only Time and Material Rates" means actual direct variable costs consistent with expense policies Approved by the Joint Executive Committee and actual direct verifiable labour costs comprised of salary and direct benefit costs, calculated as a daily rate, and in all cases, without any mark-up thereon.

"Critical Issues" has the meaning given to it in Section 6.3 (*Initial and Working Transformation Plan*).

"Custody" means to have physical possession and immediate responsibility for the safe-keeping, preservation and protection of a Record.

"Dedicated Assets" means all tangible assets and equipment (and for greater clarification, other than Software), that are then being used by the Service Provider on a seventy-five percent (75%) or greater dedicated basis in the provision of the Services to the Province, and such other tangible personal assets or equipment that are not so dedicated which the Parties mutually agree should constitute a "Dedicated Asset".

"Deficiency" means:

(a) a misstatement or misrepresentation by the Service Provider in its reporting, accounting or record keeping pursuant to this Agreement;

(b) a failure by the Service Provider to comply with the provisions of GAAP when required to do so;

(c) a failure by the Service Provider to comply with the provisions of this Agreement (including the performance of the Services);

(d) a failure by the Service Provider to comply with the Province Policies, Applicable Laws, or any other applicable requirements of regulatory bodies and authorities having competent jurisdiction (other than a failure to comply with a Disclosure Order);

(e) the occurrence of any fraud, malfeasance or wilful misconduct by the Service Provider in the performance of the Services; or

(f) any material deficiency identified in an audit report, a report prepared consistent with GAAP, or a SysTrust Report.

"Designated Contracts" means the Subcontracts, contracts with Suppliers, and Software licenses and other contracts that the Province determines, in consultation with the Service Provided, to have assigned to, and assumed by, either the Province, the Alternative Service Provider, or a combination of the two, in connection with the Termination of this Agreement.

"Directive" has the meaning given to it in Section 11.4 (*Province Right to Issue Directives*).

"Disaster" means any event or circumstance that adversely affects or disrupts (or has the potential to adversely affect or disrupt) the Services, or the ability of the Service Provider or its Subcontractors to otherwise comply with the terms of this Agreement or to otherwise operate their businesses, whether within or outside the control of the Service Provider including, without limitation, any Force Majeure Event or Labour Disruption.

"Disclosure Order" has the meaning given to it in Section 16.2 *(Foreign Disclosures)*.

"Dispute" means a dispute, claim, question, difference or disagreement between the Parties arising out of or related to the Services or the Agreement.

"Dispute Resolution Process" means the informal and formal process established under Article 27 (*Dispute Resolution*) for the resolution of Disputes.

"Documentation" means the Manuals and other documentation regarding the capabilities, implementation, installation, operation, application, use or method of performance of that which is being documented, including, as applicable and available, user manuals, business process maps, functional specifications, technical specifications, systems operations manuals, console operations manuals, linking instructions, error logs and reports, scripts, forms, templates, and other manuals and reports, whether in printed or electronic format.

"Economic Model" means the specific economic model prepared jointly by the Parties in connection with this Agreement, the final form of which is dated for reference as of the Effective

Date, and is represented in electronic Excel format, a hard copy of which is signed by the Parties on such date.

"Effective Date" has the meaning give to it in the first paragraph of this Agreement.

"Event of Insolvency" means the occurrence of any one of the following events regarding the Service Provider, the Performance Guarantor or the Financial Guarantor, and Persons who have Corporate Control of them:

(a) if such Person:

(i) other than in connection with a bona fide corporate reorganization which does not otherwise contravene this Agreement, is wound up, dissolved, liquidated or has its existence terminated or has any resolution passed therefor or makes a general assignment for the benefit of its creditors or a proposal under any present or future law relating to bankruptcy, insolvency, or other relief for or against debtors generally, domestic or foreign, including the *Bankruptcy and Insolvency Act* (Canada),

(ii) makes an application to the applicable court for a compromise or arrangement under any present or future law relating to bankruptcy, insolvency, or other relief for or against debtors generally, domestic or foreign, including the *Companies' Creditors Arrangement Act* (Canada), or

(iii) files any written request, application, answer or other document seeking or consenting to any re-organization, arrangement, composition, re-adjustment, liquidation or similar relief for itself under any present or future law relating to bankruptcy, insolvency, or other relief for or against debtors generally, domestic or foreign, including any notice of intention to make a proposal pursuant to the *Bankruptcy and Insolvency Act* (Canada);

(b) if a court of competent jurisdiction enters an order, judgment, or decree against such Person which approves or provides for any reorganization, arrangement, composition, re-adjustment, liquidation, dissolution, winding up, termination or existence, declaration of bankruptcy or insolvency or similar relief with respect to such Person, under any present or future law relating to bankruptcy, insolvency, or other relief for or against debtors generally and such order, judgment, or decree remains un-vacated and un-stayed for an aggregate period of sixty (60) days (whether or not consecutive) from the date it is made;

(c) if any trustee in bankruptcy, receiver, receiver and manager, liquidator or any other officer with similar powers is appointed for or with respect to such Person and that appointment remains in effect for an aggregate period of sixty (60) days (whether or not consecutive) from the date of the appointment; or

(d) if an encumbrance or anyone acting on behalf of an encumbrancer takes possession of all or substantially all of the property of such Person and remains in possession for an aggregate period of sixty (60) days (whether of not consecutive) from the first date of the taking of possession.

"Extension" has the meaning given to it in Section 2.7 *(One Year Extension)*.

"External Personnel" has the meaning given to it in Section 11.9 *(General Principles Regarding Personnel)*.

"External Personnel Agreement" has the meaning given to it in Section 12.5 *(Non-Disclosure Documents)*.

"Fees" means the fees set out in **Schedule 23** *(Fees)* that are payable by the Province to the Service Provider in consideration for the provision of the Services pursuant to the terms of this Agreement.

"Final Hand-Over Date" has the meaning given to it in Section 3.11 *(Delays Caused by Service Provider)*.

"Financial Guarantee" means an irrevocable and unconditional guarantee of certain liabilities of the Service Provider under this Agreement, to be provided by the Financial Guarantor in the form attached to this Agreement as **Schedule 33** *(Financial Guarantee)*.

"Financial Guarantor" means •.

"Force Majeure Event" means the occurrence of one or more of the following events that is beyond the reasonable control of a Party, and that interferes with, delays or prevents performance of the obligations of a Party under this Agreement, provided that the non-performing Party is without fault in causing or failing to prevent such occurrence, and such occurrence cannot be circumvented through the use of reasonable alternative sources, workaround plans or other similar means (including, with respect to the Service Provider, by the Service Provider meeting its business continuity and disaster recovery obligations described in this Agreement), and includes the following:

(a) explosions, fires, floods, earthquakes, catastrophic weather conditions or other elements of nature or acts of God;

(b) acts of war (declared or undeclared), acts of terrorism, insurrection, riots, civil disorders, rebellion or sabotage;

(c) failures or fluctuations in electrical power or telecommunication services or other similar public utilities; and

(d) other events which the Parties expressly agree in writing as constituting a "Force Majeure Event".

For greater clarification, a "Force Majeure Event" will specifically exclude: (1) any Labour Disruption; (2) lack of financial capacity; and (3) and any non-performance or other similar failure on behalf of a Subcontractor or Supplier unless such non-performance or similar failure results from of one or more of the events described in paragraphs (a) to (d) above that is beyond the reasonable control of the Subcontractor or Supplier, and that interferes with, delays or prevents performance of the obligations of the Subcontractor or supplier, provided that the non-performing Subcontractor or supplier is without fault in causing or failing to prevent such occurrence, and such occurrence cannot be circumvented through the use of reasonable alternative sources, workaround plans or other similar means.

"Foreign Disclosure Laws" means any laws, statutes, by-laws, treaty, directive, policy having the force of law, order, judgment, injunction, award, decree or other similar matter of any government, legislature (or similar body), court, governmental department, commission, board, bureau, agency, instrumentality, province, state, territory, association, county, municipality, city, town or other political of governmental jurisdiction, whether not or in the future constituted, outside of Canada, that may require, request, or otherwise demand access, use or disclosure of Personal Information, whether to intercept or obstruct terrorism, or for any other reason.

"Foreign Employed Individual" means individuals who have entered into an employment agreement or other similar agreement for the provision of personal services thereunder, whether express or implied by law, with a Person that is not a Canadian Entity.

"FTE" means, with respect to personnel recourses, a full-time equivalent employee working 1,470 hours per year.

"GAAP" has the meaning given to it in Section 1.6 *(Accounting Policy)*.

"Governmental Authority" means any court or governmental department, commission, board, bureau, agency, or instrumentality of Canada, or of any province, state, territory, county, municipality, city, town, or other political jurisdiction, whether domestic or foreign, and whether now or in the future constituted or existing, having competent jurisdiction over the business that is the subject of the Services or over any Party to this Agreement.

"Governance Process" means the interactions between the Parties through the established governance channels and processes described in **Schedule 18** *(Governance)*, as applicable.

"GST" means the tax imposed under Part IX of the *Excise Tax Act* (Canada), as the same may from time to time be amended or replaced.

"Guarantees" means the Performance Guarantee and the Financial Guarantee.

"Hand-Over Date" means •, as such date may be changed in accordance with Article 3 (*Initial Transition*).

"Impact Assessment" has the meaning given to it in Subsection 7.8(d) (*Implementation of Mandatory Changes*).

"Indemnified Party" has the meaning given to it in Subsection 25.3(a) (*Third Party Claim Process*).

"Indemnifying Party" has the meaning given to it in Subsection 25.3(a) (*Third Party Claim Process*).

"Initial Term" means the initial term of this Agreement, as more particularly described in Section 2.1 *(Initial Term)*.

"Intellectual Property" means intellectual property, industrial and intangible of whatever nature and kind in any jurisdiction, including software, trademarks, official marks, brand names, business names, trade names, domain names, trading styles, logos, trade secrets, inventions, innovations, discoveries, research, processes, developments, formulae, product formulations, compositions of matter, databases, works of authorship, works subject to copyright, guides,

manuals and designs, and including Modifications to any of the foregoing, in all cases whether patented or patentable, whether registered or unregistered, and in any medium whatsoever.

"Intellectual Property Rights" means any and all rights in respect of, in or to Intellectual Property, whether pursuant to statute, common law or other laws, including any and all:

(a) rights in respect of trademarks and trade names;

(b) copyrights and the benefit of any waivers of moral rights;

(c) database rights;

(d) rights in respect of industrial designs, integrated circuit topographies, and mask works;

(e) patents and patent applications;

(f) rights and obligations in respect of trade secrets; and

(g) all applications, registrations, renewals, extensions, continuations, divisions, reissues, and restorations relating to any such rights (where applicable), now or hereafter in force and effect throughout the world (including any rights in any of the foregoing).

"Joint Executive Committee" has the meaning given to it in **Schedule 18** *(Governance)*.

"JSD Agreement" means the Joint Solution Definition Agreement dated **[insert date]** between the Province and **[insert name of successful proponent, which should either by the Service Provider or the Performance guarantor]**.

"JSRFP" means the Joint Solution Request for Proposal as posted to BC Bid on **[June 19, 2007]** attached as **Schedule 40** *(JSRFP)*.

"Key Positions" has the meaning given to it in Section 11.6 (*Key Positions*).

"Labour Disruption" means a labour dispute, lockout, strike or other industrial action or labour strife, whether direct or indirect and whether lawful or unlawful.

"Licensee Party" has the meaning given to it in Subsection 19.8 (*Use of Confidential Information in Licensed Rights*).

"License Termination Date" has the meaning given to it in Subsection 19.5(f) *(Use of Province Software for the Services)*.

"Licensor Party" has the meaning given to it in Subsection 19.8 (*Use of Confidential Information in Licensed Rights*).

"Liens" means any and all liens, claims, liabilities, security interests, encumbrances, pledges, mortgages or charges of any kind whatsoever.

"Manager" means a person who has another individual or other individuals reporting to him or her.

"Mandatory Change" has the meaning given to it in Section 7.7 (*Mandatory Changes*).

"Mandatory Change Request" has the meaning given to it in Section 7.8 (*Implementation of Mandatory Changes)*.

"Master Transfer Agreement" means the Master Transfer Agreement of even date between the Province and the Service Provider.

"Material Breach" has the meaning given to it in Section 28.1 (*Service Provider Material Breach*).

"Material Infrastructure Changes" has the meaning given to it in Section 20.5 (*Material Changes to the Province Shares Infrastructure*).

"Material Services" means • **[NOTE – to be defined]**.

"Material Subcontract" has the meaning given to it in Section 12.8 (*Material Subcontractors*).

"Material Subcontractor" means any Subcontractor who is a party to a Material Subcontract.

"Maximum Credit Amount" has the meaning given to it in **Schedule 11** *(Service Levels)*.

"Mediation Notice" has the meaning given to it in Subsection 27.1(e) (*Informal Dispute Resolution*).

"Ministry" means the Ministry of Labour and Citizens' Services of the Province of British Columbia, and any successor thereto.

"Modifications" means all corrections, modifications, enhancements, improvements, supplements or derivative works, and includes interface applications in connection with any Software.

"New Records" means any Record created by the Service Provider or its Subcontractors in the performance of the Services which contains Province Confidential Information or Personal Information or other similar types of Records relating to the Services performed by the Service Provider, and for greater clarification does not include any Records created or maintained by the Service Provider for internal or management purposes which do not contain any Province Confidential Information or Personal Information.

"Non-Compliance" means a deliverable in respect of the Transformation not being in compliance with the Transformation Plan, or that Critical Issues in respect of such deliverable are not adequately addressed, as determined by the Province.

"Ordinary Course Changes" has the meaning given to it in Section 7.1 *(Ordinary Course Changes)*.

"Partial Commencement" has the meaning given to it in Section 3.11 *(Delays Caused by Service Provider)*.

"Parties" means the Service Provider and the Province, and **"Party"** means either one of them, as applicable.

"Performance Guarantee" means an irrevocable and unconditional guarantee of the performance and satisfaction of all liabilities and obligations of the Service Provider under this Agreement to be provided by the Performance Guarantor, in the form attached as **Schedule 32** *(Performance Guarantee)*.

"Performance Guarantor" means •.

"Person" means any natural person, corporation, division of a corporation, partnership, joint venture (which includes a co-ownership), association, company, estate, unincorporated organization, society, trust, government, agency or Governmental Authority.

"Personal Information" means all recorded information that:

(a) is about an identifiable individual or is defined or deemed as "personal information" pursuant to any laws or regulations related to privacy or data protection that are applicable to the Province or to the Service Provider (including, without limitation, any information that constitutes "personal information" as such term is defined, from time to time, pursuant to the *Freedom of Information and Protection of Privacy Act* (British Columbia)); and

(b) is transferred to, collected or compiled by, or is otherwise under the Custody, Control or possession of the Service Provider in connection with or as a result of performing the Services under this Agreement, or is otherwise held by the Service Provider on behalf of the Province.

"Personnel" has the meaning given to it in Section 11.9 *(General Principles Regarding Personnel)*.

"Privacy Impact Assessment" means a review of processes, procedures and practices to ensure that Personal Information is collected, managed, stored and protected in accordance with the applicable privacy legislation, policies and commitments (including the *Freedom of Information and Protection of Privacy Act* (British Columbia)).

"Privacy Obligations" has the meaning given to it in Section 16.1 *(Privacy Obligations)*, and as more fully set forth in **Schedule 24** *(Privacy Obligations)*.

"Problem" has the meaning given to it in Section 8.8 *(Problem Alert and Escalation Procedures)*.

"Problem Management Procedures" has the meaning given to it in Section 8.8 *(Problem Alert and Escalation Procedures)*.

"Proposal" has the meaning given to it in Subsection 7.5(b) *(Change Request Process)*.

"Proprietary Software" has the meaning given to it in Section 19.8 (*Use of Confidential Information in Licensed Rights*).

"Province Confidential Information" means any technical, business, financial, personal, employee, operational, scientific, research or other information or data of the Province, and any other information regarding the Province's business, plans and markets, information of or relating to the Province's customers and Stakeholders, or of any Person that has disclosed such

information to the Province or its agents, in whatsoever form or media, whether in writing, in electronic form or communicated orally or visually, that, at the time of disclosure is designated as confidential (or like designation), or by its sensitive nature should be treated as confidential, or if it were information of the Service Provider, would be treated as confidential information by the Service Provider, and including any Personal Information, the Province Proprietary Software, and all information or data with respect to the Province Records, whether or not designated as confidential (or like designation).

"Province Indemnified Parties" has the meaning given to it in Section 25.2 (*Indemnification by the Service Provider*).

"Province Intellectual Property" means all Intellectual Property and all Intellectual Property Rights of the Province including, without limitation, those referred to in this Agreement, and those owned or otherwise acquired by the Province before or after the execution of this Agreement, whether or not specifically referred to in this Agreement.

"Province Licensed Software" means •.

"Province Material Breach" has the meaning given to it in Section 28.3 (*Material Breach by Province*).

"Province Marks" has the meaning given to it in Section 10.1 *(Province Marks)*.

"Province Policies" means the policies of the Province from time to time, including without limitation the Province's accounting policy, the policies referenced in the attached **Schedule 28** *(Specific Laws and Policies)* (copies of which have been provided to the Service Provider), and other governmental policies relating to reporting or data and record keeping, but excluding policies regarding human resource management.

"Province Proprietary Software" means the Software owned by or licensed to the Province (and which the Province has the right to authorize the Service Provider to use in the manner specified in Article 19 *(Intellectual Property and Proprietary Rights)*, including object and source code versions, and any Documentation and any Modifications or interfaces relating to the foregoing created by or on behalf of the Province from time to time, but excluding Third Party Software.

"Province Records" means all Records containing Personal Information of the Province or the Province customers, and all Personal Information relevant to the performance of the Services and other transactions contemplated in this Agreement, or any other Province Confidential Information, and includes any Transferred Records and New Records.

"Province Shared Infrastructure" means those parts or components of certain Systems owned and operated by the Province, or on behalf of the Province by third party Persons, which are required by the Service Provider to support the delivery and performance of the Services, and which Systems are shared resources of the Province used to support other services and other uses by the Province as well, as such Systems are expressly and specifically listed in **Schedule 41** *(Province Shared Infrastructure)*, as such Schedule may be amended or updated by the Parties from time to time.

"Province Trust Rights" has the meaning given to it in Subsection 19.3(b) (*Assignment by Service Provider*).

"PST" means all applicable provincial sales or service taxes payable in pursuant to the *Social Services Tax Act* (British Columbia) as the same may from time to time be amended or replaced.

"Publicity Materials" has the meaning given to it in Section 10.4 (*Publicity*).

"Records" means books, records, reports, documents, maps, drawings, correspondence, system logs, system development records, accounts, invoices, backup data (including original source documents) and other similar documents, images, writings or information by any means whether graphic, electronic, audio, mechanical or otherwise.

"Recovery Time Objective" means the maximum acceptable period of time that can elapse before a disruption in Services is remedied in order to prevent the occurrence of material adverse effects as a result thereof, consisting of:

(a) the period of time between the occurrence of a disruption and the declaration of a Disaster in connection with the disruption; and

(b) the period of time from the declaration of a Disaster to the completion of the steps and actions required to be undertaken in respect of the Disaster in accordance with the Business Continuity Plan or the Disaster Recovery Plan, and the resumption of the delivery of the Services in the ordinary course as a result of the implementation of the Business Continuity Plan or the Disaster Recovery Plan.

"Renewal Agreement" has the meaning give to it in Section 2.6 *(Renewal Negotiations)*.

"Renewal Term" has the meaning given to it in Section 2.4 *(Renewal Option)*.

"Retained Employees" has the meaning given to it in Section 29.9 (*Province Severance Costs*).

"Service Centre" means the permanent facilities from where the Service Provider will perform the majority of the Services, having an address as set forth in **Schedule 8** *(Service Locations)*, the location of which is subject to change in accordance with the provisions of Section 5.3 (*Relocation of the Service Provider Service Locations*).

"Service Level Credits" has the meaning given to it in Section 8.9 (*Service Level Credits*).

"Service Level Requirements" means those Service Levels to which a Weighting is attached, as indicated in **Schedule 11** *(Service Levels)*, and for which the Province has attached a Service Level Credit in accordance with the provisions of Article 8 (*Service Levels*), and for greater clarification, no Weighting attached thereto may be less than one percent (1%).

"Service Levels" means the service measurement concepts and criteria, and corresponding performance level targets to be achieved by the Service Provider in performing the Services, as set forth and described **Schedule 11** *(Service Levels)*, as may be amended from time to time in accordance with this Agreement.

"Service Level Termination Event" has the meaning given to it in **Schedule 12** (*Service Level Failures)*.

"Service Locations" means has the meaning given to it in Section 5.2 (*Service Locations*).

"Service Provider" has the meaning given to it in the first paragraph of this Agreement.

"Service Provider Confidential Information" means any technical, business, financial, personal, employee, operational, scientific, research or other information or data in whatsoever form or media, whether in writing, electronic form or communicated orally or visually that, at the time of disclosure is designated as confidential (or like designation), or by its sensitive nature should be treated as confidential, or if it were information of the Province, would be treated as confidential information by the Province, and the Service Provider's financial information, purchasing and cost information, price and cost data, (other than information that is contained in the Project Summary Report but only to the extent and level of detail contained in the Project Summary Report. Notwithstanding the foregoing, the "the Service Provider Confidential Information" will exclude all Province Confidential Information, whether or not expressly indicated for exclusion.

"Service Provider Group" has the meaning given to it in Subsection 33.13(d) (*Governing Law*).

"Service Provider Mark" has the meaning given to it in Section 10.3 (*Service Provider Marks*).

"Service Provider Software" means the Software owned by the Service Provider or its Affiliates on the Hand-Over Date, or which it or its Affiliates develops or acquires after the Hand-Over Date independent of this Agreement, including object and source code versions, Documentation and any Modifications or interfaces relating to the foregoing, created by or on behalf of the Service Provider from time to time, and that are used in the provision of the Services and which do not constitute Province Proprietary Software or Third Party Software.

"Services" has the meaning given to it in Section 4.1 (*Overview of Services*).

"Severance Amount" means an amount payable to an individual in connection with the cessation of employment of such individual and includes amounts for severance, layoff, termination notice or any other similar amounts related to or arising in connection with the cessation of employment and whether required by law, at equity, or under the terms of any agreement governing the employment of such individual including a collective agreement, or otherwise.

"Shared Infrastructure Use Period" has the meaning given to it in Section 20.2 (*Use of Province Shared Infrastructure*).

"Software" means software applications, software tools, methodologies and computer programs, including all versions thereof, and all related documentation, manuals, program files, data files, computer related data, field and data definitions and relationships, data definition specifications, data models, program and system logic, program modules, routines, sub-routines, algorithms, program architecture, design concepts, system designs, program structure, sequence and organization, screen displays and report layouts, technology and techniques, object code (and if obtained, source code) and interfaces.

"Source Code" means the human-readable form of a computer instruction, including related system documentation, applicable comments and procedural codes such as job control language.

"Source Materials" means, in relation to items of Software, supporting materials that would enable a reasonable skilled programmer to compile, debug and support and/or make improvements to such software in a commercially reasonable manner including (i) any Source Code related thereto, reasonably annotated, (ii) technical and system documentation including

detailed design, functional, operational, and technical documentation, flow charts, diagrams, file layouts, report layouts, screen layouts, business rules, data and database models and structures, working papers and reasonably related notes and memoranda in electronic or written format, which were made or obtained in relation to the design and development of such software and compilation instructions related to such software, (iii) listing by name, version and vendor of relevant third Persons' compliers, utilities and other software that are necessary for normal operation of such software to which the Source Materials related including sufficient information to procure a license from such vendors, (iv) a detailed listing of relevant equipment and information necessary for normal operation of such software, and (v) all other information reasonably necessary to rebuild, install, and otherwise implement the Software in the context of the applicable System(s) including, without limitation, all relevant tools, programs, files, encryptions keys, make files, installation instructions, systems settings, and database settings.

"Stage" means each stage of the Transformation as set out in the Transformation Plan.

"Stakeholders" means any Person that exchanges data with the Province, relies on the Services or has a direct material stake in the delivery of the Services other than Province customers, including without limitation, the Broader Public Sector and **[insert as applicable to the transaction]**.

"Subcontract" means a contract entered into between the Service Provider and a Subcontractor, but does not include Supplier Agreements.

"Subcontractor" means any third party Person engaged by the Service Provider to perform any of the Services on behalf of the Service Provider, and includes a Material Subcontractor and an Assigned Subcontractor, but does not include a Supplier.

"Supplier" means a third party supplier for the delivery and provision of non-material and ordinary course goods and services relating to or in connection with the Services contemplated by this Agreement, but expressly excluding Subcontractors.

"Standard Time and Materials Rates" means actual direct variable costs consistent with expense policies Approved by the Joint Executive Committee, and actual direct verifiable labour costs comprised of salary and direct benefit costs, calculated as a daily rate, with a •% overhead margin applied to all of the foregoing.

"Systems" means the hardware, equipment, software and communications equipment which is required or otherwise used in the performance of the Services.

"SysTrust Report" has the meaning given to it in Section 22.6 (*SysTrust Report*).

"Taxes" mean any and all taxes, fees, levies, or other assessments, including federal, state, local, or foreign income, capital, profits, excise, real or personal property, sales (including PST), withholding, social security, occupation, use, services, value added (and for greater clarification, including GST and PST), license, net worth, payroll, franchise, severance, stamp, transfer, registration, premium, windfall, environmental, customs duties, unemployment, disability, or any similar taxes imposed by any Taxing Authority together with any interest, penalties or additions to tax and additional amounts imposed with respect thereto (including any fee or assessment or other charge in the nature of or in lieu of any tax) in each case, whether imposed by law or otherwise, and any liability in respect of any tax as a result of being a member of any affiliated, consolidated, combined, unitary or similar group.

"Taxing Authority" means any multinational, national, federal, state, provincial, local, municipal or other government (including any governmental agency, branch, department, official, entity, court or other tribunal and any body exercising, or entitled to exercise, any administrative, executive, judicial, legislative, regulatory or taxing authority or power of any nature) responsible for the imposition or collection of any Taxes.

"Term" means the Initial Term of this Agreement and any Renewal Term or Extension, as applicable.

"Termination" means the expiry or earlier termination of this Agreement pursuant to the provisions of this Agreement.

"Termination Assistance Period" has the meaning given to it in Section 29.1 (*Termination Services*).

"Termination Assistance Plan" has the meaning given to it in Section 29.2 (*Termination Assistance Plan*).

"Termination Date" means the effective date of the expiry or earlier termination of the Initial Term, the Renewal Term or the Extension, as applicable.

"Termination Licensed Software" has the meaning give to it in Subsection 29.1(i) (*Termination Services*).

"Termination Notice" means a written notice terminating this Agreement given by one Party to the other in accordance with the terms of this Agreement.

"Termination Services" has the meaning given to it in Section 29.1 (*Termination Services*).

"Third Party Software" has the meaning given to it in Section 19.9 (*Third Party Software*).

"Transaction Documents" means, collectively, this Agreement, the Master Transfer Agreement, the Guarantees and **[insert description of other material documents to be tabled at closing]**

"Transferred Records" means those Records transferred by the Province to the Service Provider under the terms of this Agreement.

"Transformation" means the orderly transition of the Services from the form of Services contemplated on the Hand-Over Date to the form of Services set forth in the Transformation Plan.

"Transformation Credits" has the meaning given to it in Section 6.7 (*Delay in Completion of Transformation*).

"Transformation Plan" has the meaning given to it in Section 6.2 (*Transformation Plan*).

"Transformed Services" has the meaning given to it in Subsection 4.1(c) (*Overview of Services*).

"Transition" has the meaning given to it in Section 3.2 (*Hand-Over of Services*).

"Transition Governance Process" has the meaning given to it in Section 3.5 (*Transition Management*).

"Transition Management Team" has the meaning given to it in Section 3.5 (*Transition Management*).

"Transition Period" means the period of time from the Effective Date until the Hand-Over Date.

"Transition Plan" has the meaning given to it in Section 3.3 (*Transition Services*).

"Transition Services" has the meaning given to it in Section 3.3 (*Transition Services*).

"Work-in-Progress Projects" means those projects described in the attached **Schedule 4** *(Work-in-Progress Projects)* that are not completed by the Province prior to the Hand-Over Date.

SCHEDULE 27

GAINSHARING

1. Purpose.

The purpose of this Schedule 27 (*Gainsharing*) is to describe the agreement between the Province and the Service Provider regarding the future growth and opportunities under STMS, in particular, future opportunities that bring benefit to both Parties as set forth in Section 3 (*Principles*) below.

2. Definitions.

Capitalized words used in this Schedule 27 (*Gainsharing*) shall have the meanings given to such words in the Agreement. In the event that a term is not defined in the Agreement, it shall have the meaning provided in Section 1 of this Schedule or in the body of this Schedule.

"Adjusted Capacity Reservation" has the meaning given to it in Schedule 23 (*Fees*).

"Capacity Reservation" has the meaning given to it in Schedule 23 (*Fees*).

"Excluded Entities" means customers of the Service Provider other than Broader Public Sector entities.

"Province Adjusted VA Commitment" has the meaning given to it in Schedule 23 (*Fees*).

"Province VA Commitment" has the meaning given to it in Schedule 23 (*Fees*).

"VA" has the meaning given to it in Schedule 23 (*Fees*).

"VA Unit Price" has the meaning given to it in Schedule 23 (*Fees*).

3. Principles.

3.1 *Future Opportunities*. The Parties shall pursue, in accordance with Schedule 26 (*Growth and Marketing*), future opportunities that bring benefit to both Parties including, without limitation, opportunities to leverage the Services under the Agreement, gaining economies of scale, and taking advantage of the aggregated volume pricing benefits for the Services (as more particularly described in Schedule 23 (*Fees*)).

3.2 *Broader Public Sector.* The Parties will proactively identify and encourage, in accordance with Schedule 26 (*Growth and Marketing*), Broader Public Sector to participate in the STMS either as Clients of WTS or Buyers of Services as contemplated under this Agreement.

4. Gainsharing.

Subject to Section 3 of Schedule 26 (*Growth and Marketing*), the Parties acknowledge and agree that any and all VA capacity reservation or adjusted capacity reservation of any Broader Public Sector, relating to or in connection with the STMS Data Centres, shall be counted toward the Province VA Commitment or Province Adjusted VA Commitment, as the case may be, and for

the purposes of determining the VA Unit Price for all Buyers. For greater certainty, the amount of any VA capacity reserved or acquired by the Excluded Entities, within the STMS Data Centres if any, shall not be counted toward the Province VA Commitment or Province Adjusted VA Commitment.

SCHEDULE 28

SPECIFIC LAWS AND POLICIES

Specific Laws

The following is a list of specific Applicable Laws applicable to the Service Provider: (a) as a service provider to the Province; and (b) as applicable in the performance of the Services.

1. *Financial Administration Act*
2. *Budget Transparency and Accountability Act*
3. *Ombudsman Act*
4. *Freedom of Information and Protection of Privacy Act*
5. *Personal Information Protection and Electronic Documents Act*
6. *Personal Information Protection Act*
7. Sections 10.1 and 10.7 of the *Health Care Act*
8. *E Health Personal Information Protection Act*

Province Policies

The following is a list of Province Policies applicable to the Service Provider: (a) as a service provider to the Province; and (b) as applicable in the performance of the Services.

As the Province Policies may be updated from time to time, the Service Provider's implementation of, and compliance with, any changes to the foregoing will be completed in accordance with the Change Order process or the Governance Process, as applicable.

1. Chapters 12, 14, 15, 16 and 20 of the Core Policy and Procedures Manual and Chapter 12 Supplemental
2. IT Asset Disposal Policy
3. Freedom of Information and Protection of Privacy Policies and Procedures Manual
4. Information Security Policy (June 2006)
5. Operational Records Classification Schedules/Administrative Records Classification Schedules (ORCs/ARCs)
6. Risk Management - Security Standards and Guidelines
7 Transparency Policy
8. IM/IT Standards Manual, The Architecture and Standards Development Lifecycle and IM/IT Strategic Initiatives and Infrastructure
9. Physical Security Standards
10. Records Management Policies
11. SEP Architecture
12. OCIO Information Security Branch
13. Section 09 – Policy Statement – Standards of Conduct (Human Resources Policies)
14. Standards of Conduct for Public Service Employees Engaged in Government Procurement Processes

SCHEDULE 29

ADDITIONAL REPRESENTATIONS AND WARRANTIES

Nil

SCHEDULE 30

INDEMNIFICATION MATTERS

(Section 25.2)

1. Indemnification by the Service Provider.

Pursuant to Section 25.2 (*Indemnification by the Service Provider*) and without duplication of any liquidated damages to be paid by the Service Provider to the Province hereunder, the Service Provider will indemnify and save harmless the Province Indemnified Parties to the fullest extent permitted by law, from and against any and all Claims suffered or incurred by any one or more of the Province Indemnified Parties arising as a result of or in connection with any of the following (except to the extent suffered or incurred as a result of or in connection with the wilful misconduct, fraud, malfeasance or gross negligence of the Province Indemnified Parties):

(a) the failure of the Service Provider to perform its obligations under any license, lease or other agreement:

(i) between the Service Provider and a third party, including Subcontractors and landlords, or

(ii) assigned by the Service Provider to the Province or to the Alternative Service Provider in connection with Termination of this Agreement, but only with respect to any Claims that arise from or relate to the period prior to the assignment thereof by the Service Provider to the Province or the Alternative Service Provider,

or any third party Claim relating thereto that arises as a result of the Province receiving Services under this Agreement;

(b) the failure of the Service Provider to perform its obligations under any Assigned Contract after the assignment thereof from the Province to the Service Provider;

(c) the failure of the Service Provider to pay and discharge any Taxes for which the Service Provider is responsible pursuant to this Agreement and all Applicable Laws (provided that nothing in the Agreement or any Transaction Document shall impose on the Service Provider any obligation or liability with respect to Taxes for which its Subcontractors may be responsible at law);

(d) the gross negligence or wilful misconduct or malfeasance of the Service Provider, its Personnel or its Subcontractors or External Personnel with respect to the Services or this Agreement;

(e) the fraud by the Service Provider, its Personnel or its Affiliates, Subcontractors or their External Personnel;

(f) the death of or bodily injury to any third party or to any employee of the Province to the extent caused by the gross negligence or wilful misconduct of the Service Provider, its Personnel or its Subcontractors or External Personnel;

(g) the loss of or damage to any tangible personal or real property of the Province, to the extent caused by the gross negligence or wilful misconduct of the Service Provider, its Personnel or its Subcontractors or External Personnel;

(h) the loss of or damage to any tangible personal or real property of any third party, to the extent caused by the gross negligence or wilful misconduct of the Service Provider, its Personnel or its Subcontractors or External Personnel;

(i) the Service Provider acting outside of the scope of the authority granted to it under the terms of the Agreement or the Service Provider's breach of the standard of care under the Agreement; and

(j) any Claim, proceeding or action taken or initiated by any member of the Service Provider Group in breach of Article 27 (*Dispute Resolution*) or Section 32.13 (*Governing Law*).

For greater clarification, the Service Provider shall not be required to indemnify the Province Indemnified Parties under this Section in respect of those Service Provider Material Breaches for which the Parties have agreed the Service Provider will pay liquidated damages under the provisions of this Agreement.

2. Indemnification by the Province.

Pursuant to Section 25.3 (*Indemnification by the Province*) the Province will indemnify and save harmless the Service Provider Indemnified Parties to the fullest extent permitted by law, from and against any and all Claims suffered or incurred by any one of more of the Service Provider Indemnified Parties arising as a result of or in connection with any of the following (except to the extent suffered or incurred as a result of or in connection with the wilful misconduct, fraud, malfeasance or gross negligence of the Service Provider Indemnified Parties):

(a) the death of or bodily injury to any third party or any employee of the Service Provider or its Affiliates to the extent caused by the gross negligence or wilful misconduct of the Province;

(b) the loss of or damages to any tangible personal or real property of the Service Provider or any tangible personal or real property of any third party to the extent caused by the gross negligence or wilful misconduct of the Province;

(c) the exercise by the Province of its right to replace the Service Provider's employees with the Province's employees pursuant to **Schedule 24** *(Privacy Obligations)*;

(d) any third party Claims brought against the Service Provider Indemnified Parties as a result of the acts or omissions of the Service Provider Indemnified Parties in reliance upon any directives or instructions issued to the Service Provider by the Province, or the compliance by the Service Provider Indemnified Parties with the written policies and procedures issued by the Province pursuant to Section 11.4 *(Province's Right to Issue Directives)* (provided that such compliance does not involve any grossly negligent acts or omissions, wilful misconduct or malfeasance of the Service Provider in implementing the same);

(e) with respect to any inspectors, investigators or auditors or representatives used by the Province in the course of an inspection, investigation or audit carried-on by the Province under Article 22 (*Audit Rights*), the failure of such inspectors, investigators or auditors to

comply with the provisions of Article 22 (*Audit Rights*) or any non-disclosure agreement entered into with the Service Provider in connection therewith;

(f) with respect to any contractors, professional advisors, agents or other third parties who have entered into a Non-Disclosure Agreement in accordance with the provisions of the Agreement or any Transaction Document, the failure of such contractors, professional advisors, agents or other third parties to comply with the provisions thereof; and

(g) with respect to any third parties to whom the Province discloses Service Provider Confidential Information pursuant to Section 16.8 (*Province Permitted Disclosure*) in order to prevent any actual or reasonably anticipated disclosure of Personal Information, any disclosure or use by such third parties of the Service Provider Confidential Information that is not required to prevent such actual or reasonably anticipated disclosure of Personal Information or to report to the Province thereon.

3. Service Provider Intellectual Property Indemnification.

Subject to 25.4 (*Third Party Claim Process*), the Service Provider will indemnify and save harmless, to the fullest extent permitted by law, the Province Indemnified Parties from and against any and all Claims suffered or incurred by them arising as a result of, or in connection with, any actual or alleged infringement by the SP Affiliate Bespoke Software, SP Affiliate Commercial Software, SP Leveraged Software, SP Licensed Software, SP Proprietary Software or the Service Provider Confidential Information of the Intellectual Property Rights of a third party (an "**SP Infringement Claim**"). Notwithstanding the foregoing, the Service Provider shall have no liability under this Section for any SP Infringement Claim if and to the extent that such SP Infringement Claim would not have arisen but for:

(a) the use by the Service Provider of any Province Intellectual Property, Province Licensed Software, Province Proprietary Software or Province Confidential Information in accordance with the provisions of this Agreement permitting the use of the same, provided that this subsection 3(a) will not apply if the SP Infringement Claim arises out of, relates to, or is caused by a Modification to such Province Intellectual Property, Province Licensed Software, Province Proprietary Software or Province Confidential Information made by the Service Provider or any Subcontractor unless: (i) the Modification was made as a result of an express written direction of the Province, and (ii) the SP Infringement Claim would not have occurred but for the Service Provider's compliance with that direction;

(b) a Modification made by the Province to the SP Affiliate Bespoke Software, SP Affiliate Commercial Software, SP Leveraged Software, SP Licensed Software and SP Proprietary Software or the Service Provider Confidential Information that was not expressly authorized in writing by the Service Provider; or

(c) the use by the Service Provider of any Third Party Intellectual Property provided to the Service Provider by the Province or third parties engaged by the Province, provided that this subsection 3(c) will not apply if the SP Infringement Claim arises out of, relates to, or is caused by a Modification to such Third Party Intellectual Property made by the Service Provider or any Subcontractor unless: (i) the Modification was made as a result of an express written direction of the Province, and (ii) the SP Infringement Claim would not have occurred but for the Service Provider's compliance with that direction.

Without limiting or otherwise restricting the Service Provider's liability and obligations to the Province Indemnified Parties in respect of the foregoing, if the Province's use of any Intellectual Property provided or otherwise made available by the Service Provider to the Province pursuant to this Agreement is found to be infringing the Intellectual Property Rights of a third party or, in the Service Provider's reasonable judgment is likely to be found to be infringing, then the Service Provider may (at its option and expense), either procure for the Province the right to continue using such Intellectual Property, or replace or modify such Intellectual Property to make its continued use non-infringing while providing substantially the same functionality. The obligations of the Service Provider under this Section 3 are in addition to the obligations of the Service Provider under Article 19 (*Intellectual Property and Proprietary Rights*) of the Agreement.

4. Province Intellectual Property Indemnification.

Subject to 25.4 (*Third Party Claim Process*), the Province will indemnify and save harmless, to the fullest extent permitted by law, the Service Provider Indemnified Parties from and against any and all Claims suffered or incurred by them arising as a result of, or in connection with, any actual or alleged infringement by the Province Intellectual Property, Province Licensed Software, Province Proprietary Software or Province Confidential Information of the Intellectual Property Rights of a third party (a "**Province Infringement Claim**"). Notwithstanding the foregoing, the Province shall have no liability under this Section for any Province Infringement Claim if and to the extent that such Province Infringement Claim would not have arisen but for:

(a) the use by the Province of any SP Affiliate Bespoke Software, SP Affiliate Commercial Software, SP Leveraged Software, SP Licensed Software and SP Proprietary Software or the Service Provider Confidential Information in accordance with the provisions of this Agreement permitting the use of the same, provided that this subsection 4(a) will not apply if the Province Infringement Claim arises out of, relates to, or is caused by a Modification to the SP Affiliate Bespoke Software, SP Affiliate Commercial Software, SP Leveraged Software, SP Licensed Software and SP Proprietary Software or the Service Provider Confidential Information made by the Province unless: (i) the Modification was made as a result of an express written direction of the Service Provider, and (ii) the Province Infringement Claim would not have occurred but for the Province's compliance with that direction;

(b) a Modification made by the Service Provider to the Province Intellectual Property, Province Licensed Software, Province Proprietary Software or Province Confidential Information that was not expressly authorized in writing by the Province; or

(c) the use by the Province of any Third Party Intellectual Property provided to the Province by the Service Provider or third parties engaged by the Service Provider, provided that this subsection 4(c) will not apply if the Province Infringement Claim arises out of, relates to, or is caused by a Modification to the Third Party Intellectual Property made by the Province unless: (i) the Modification was made as a result of an express written direction of the Service Provider, and (ii) the Province Infringement Claim would not have occurred but for the Province's compliance with that direction.

Without limiting or otherwise restricting the Province's liability and obligations to the Service Provider Indemnified Parties in respect of the foregoing, if the Service Provider's use of any Intellectual Property provided or otherwise made available by the Province to the Service Provider pursuant to this Agreement is found to be infringing the Intellectual Property Rights of a third party or, in the Province's reasonable judgment is likely to be found to be infringing, then the Province may (at its option and expense), either

procure for the Service Provider the right to continue using such Intellectual Property, or replace or modify such Intellectual Property to make its continued use non-infringing while providing substantially the same functionality. The obligations of the Province under this Section 4 are in addition to the obligations of the Province under Article 19 (*Intellectual Property and Proprietary Rights*) of the Agreement.

SCHEDULE 31

LIMITATION ON LIABILITY

(Section 25.5)

At issue for Inquiry

Page 1685 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
At issue for Inquiry

SCHEDULE 32

PERFORMANCE GUARANTEE

(Section 25.6)

PERFORMANCE GUARANTEE

This Guarantee is executed as of _____, by **EDS CANADA INC.**. ("**EDS Canada**"), a corporation continued under the laws of Canada with an office at 33 Yonge Street, Suite 500, Toronto, Ontario M5E 1G4, for the benefit of **HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA** (the "**Province**"), **as represented by the Minister of Labour and Citizens' Services.**

WHEREAS, EDS Advanced Solutions Inc. ("**EDS Subsidiary**"), a British Columbia corporation with a place of business at Vancouver Island Technology Park, 2200-4464 Markham Road, Victoria, British Columbia, V8Z 7X8, and the Province concurrently herewith have executed a certain Master Services Agreement (the "**Agreement**") dated as of _____ (terms capitalized in this Guarantee but not defined in this Guarantee shall have the meanings given to them in the Agreement); and

WHEREAS, as a condition to entering into the Agreement, the Province has required that EDS Canada deliver this written Guarantee of the obligations of EDS Subsidiary set forth in the Agreement and the Transaction Documents; and

NOW THEREFORE EDS Canada makes this Guarantee knowing that the Province shall rely on this Guarantee in entering into the STMS Agreements (defined below). EDS Canada conclusively acknowledges that reliance by the Province on this Guarantee is in every respect justifiable and that it received adequate and fair and valuable consideration for this Guarantee, the receipt and adequacy of which are hereby acknowledged. Subject to the terms and conditions hereof, EDS Canada hereby agrees as follows:

1. **GUARANTEE**

1.1 **Guaranteed Obligations.** For purposes of this Guarantee, "**Guaranteed Obligations**" means the performance obligations, debts and liabilities of EDS Subsidiary, of any kind and in each case arising under, pursuant to, or in connection with the Agreement or any of the other Transaction Documents (collectively, the "**STMS Agreements**").

1.2 **Performance Guarantee.** EDS Canada hereby absolutely, unconditionally and irrevocably guarantees to the Province the due performance and fulfillment by EDS Subsidiary of the Guaranteed Obligations, all in accordance with and subject to the terms and conditions of this Guarantee. If EDS Subsidiary defaults in any material respect in the performance of any of the Guaranteed Obligations (other than for reasons which result in EDS Subsidiary being excused from performing such obligations), and fails to cure such default prior to the expiration of any applicable notice or cure period, then within a reasonable period of time following EDS Canada's receipt of written notice from the Province of EDS Subsidiary's default, EDS Canada shall cause the Guaranteed Obligations to be performed, fulfilled or otherwise satisfied in accordance with the terms and conditions of the STMS Agreements and in so doing, EDS Canada shall comply with the terms of the STMS Agreements,

including Article 16 of the Agreement, as though EDS Canada were the named party therein in the place of EDS Subsidiary, and at no cost to the Province other than as provided in the STMS Agreements.

2. CONTINUING NATURE OF GUARANTEE

2.1 **Continuing and Irrevocable.** This Guarantee shall be continuing and irrevocable until the earlier to occur of: (i) satisfaction of the Guaranteed Obligations; and (ii) termination of the Agreement other that as a result of a default by EDS Subsidiary.

2.2 **Limitation of Liability.** The liability of EDS Canada under this Guarantee, including any liability of EDS Canada in connection with the STMS Agreements, shall be coextensive with, but not in excess of, the liability of EDS Subsidiary to the Province under the STMS Agreements, and EDS Canada shall be entitled to the benefit of and may assert all rights, defenses, counterclaims, and other protections to which EDS Subsidiary may be entitled with respect to any such liability, including without limitation, all provisions of the STMS Agreements relating to the limitation of liability, limitation periods with respect to Claims under the STMS Agreements and the resolution of disputes. In no event shall the aggregate liability of EDS Canada, any other Affiliate of EDS Canada who may have provided a guarantee of EDS Subsidiary's obligations and EDS Subsidiary under this Guarantee, any other such guarantee and the STMS Agreements exceed the liability of EDS Subsidiary under the STMS Agreements. Notwithstanding the foregoing, EDS Canada shall not be entitled to the benefit of the defenses, counterclaims and protections described in Section 2.3 below except to the extent that such defenses, counterclaims and protections are available to EDS Subsidiary.

2.3 **No Release.** The liability of EDS Canada under this Guarantee shall not be released, reduced, impaired or affected by or as a result of any matter or thing whatsoever that would otherwise release or discharge a guarantor or limit its obligations (except as set forth in Section 2.2 above), including any of the following:

(a) any withdrawal of any demand (including the commencement and continuance of any legal proceedings) by the Province for performance by EDS Canada of any Guaranteed Obligations under this Guarantee;

(b) if, whether or not with EDS Canada's knowledge, the Province grants extensions of time, renewals, indulgences, amendments, modifications, waivers, releases, discharges, makes any compromise or transaction or arrangement, or otherwise deals with any of the Guaranteed Obligations, the STMS Agreements, EDS Subsidiary, or with any security, guarantee or similar assurance held by it;

(c) any compromise by the Province of any of the Guaranteed Obligations or any other guarantee in respect thereof;

(d) the voluntary or involuntary liquidation, dissolution, consolidation or merger (or the sale or other disposition of all or part of the assets) of EDS Canada or EDS Subsidiary or any of their respective Affiliates;

(e) insolvency, bankruptcy, receivership, assignment for the benefit of creditors or reorganization, arrangement, composition or readjustment of debt, or other similar proceeding affecting EDS Canada, EDS Subsidiary or any of their respective Affiliates,

or any similar proceedings instituted by or against EDS Canada, EDS Subsidiary or the assets of either of them; or

(f) the failure of the Province or any other party to take, protect or preserve any rights, security, guarantee or similar assurance of EDS Subsidiary or any other Affiliate of EDS Subsidiary (other than the rights and security of EDS Subsidiary and its Affiliates referred to in Schedule 23 of the Agreement, if any), whether or not caused or resulting from any act or omission of the Province or any person acting for the Province or for whom the Province may be responsible.

3. PROCEEDINGS UNDER GUARANTEE

3.1 **Proceeding Against EDS Canada.** The Province shall not proceed against EDS Canada in respect of the Guaranteed Obligations until EDS Subsidiary shall have defaulted in a material respect in the performance of such Guaranteed Obligations (other than for reasons which result in EDS Subsidiary being excused from performing such obligations), and shall have failed to cure such default prior to the expiration of any applicable notice or cure period. The Province shall provide EDS Canada with a copy of any notice of default delivered by the Province to EDS Subsidiary at the same time as such notice of default is delivered by the Province to EDS Subsidiary. Any failure by the Province to pursue rights or remedies against any guarantor shall not relieve EDS Canada from its obligations under this Guarantee.

3.2 **Reinstatement.** This Guarantee shall be reinstated if at any time any amounts received on account of any Guaranteed Obligations must be returned by the Province upon the insolvency, bankruptcy, dissolution, liquidation or reorganization of the EDS Canada, EDS Subsidiary or any of their respective Affiliates.

3.3 **Set Off.** Any amounts owed to EDS Subsidiary by the Province under the Agreement or the Transaction Documents or otherwise in respect of the Services, but excluding any amounts under Dispute, may be set-off by EDS Canada against the Guaranteed Obligations.

4. REPRESENTATIONS, WARRANTIES AND OTHER COVENANTS

4.1 **Representations.** EDS Canada represents and warrants as follows to the Province, as of the date of this Guarantee, and acknowledges and agrees that the Province is relying on such representations and warranties and is entitled to do so in entering into this Guarantee and the STMS Agreements:

(a) EDS Canada is a company duly continued and validly existing under the laws of Canada and is in good standing with respect to the filing of annual returns thereunder, and EDS Canada is an Affiliate of Hewlett-Packard Company, a Delaware corporation;

(b) EDS Canada has all necessary power, capacity and legal authority to enter into, execute and deliver this Guarantee and to perform its obligations hereunder, and this Guarantee has been duly executed and delivered by EDS Canada, and constitutes a legal, valid and binding obligation of EDS Canada enforceable against EDS Canada in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

(c) neither the execution and delivery of this Guarantee, nor the compliance with the terms of this Guarantee by EDS Canada:

(i) has resulted or will result in a violation of any Applicable Laws;

(ii) has resulted or will result in a breach of, or constitute a default under, EDS Canada's constating documents, any shareholders' agreement to which it is a party or any shareholder or directors' resolutions, which would have a material adverse effect on EDS Canada's ability to perform its obligations under this Guarantee, or

(iii) has resulted or will result in a breach of, or constitute a default under any instrument or agreement to which EDS Canada is a party or by which EDS Canada is bound, which breach or default would have a material adverse effect on EDS Canada's ability to perform its obligations under this Guarantee.

4.2 **Taxes.** Any and all payments by EDS Canada to the Province under this Guarantee shall be made free and clear of and without deduction for any and all present or future taxes, levies, imposts, deductions, charges or withholdings, and all liabilities with respect thereto, excluding those that shall be adjusted for in accordance with this Section. If EDS Canada shall be required by law to deduct any such amounts from or in respect of any sum payable to the Province under this Guarantee, then:

(a) the sum payable shall be increased as may be necessary so that after making all required deductions (including deductions applicable to additional sums payable under this Section) the Province will receive an amount equal to the sum it would have received had no such deductions been made;

(b) EDS Canada shall make such deductions; and

(c) EDS Canada shall pay the full amount deducted to the relevant Governmental Authority in accordance with Applicable Laws.

5. **MISCELLANEOUS**

5.1 **STMS Agreements.** EDS Canada acknowledges receipt of a copy of the STMS Agreements. EDS Canada expressly agrees that: (i) the Province is not required to provide EDS Canada with, and EDS Canada hereby waives any right to receive from the Province, copies of any amendments to the STMS Agreements; and (ii) the obligations of EDS Canada to the Province under this Guarantee shall in no way be affected, diminished or otherwise limited as a result of any amendments made by EDS Subsidiary and the Province to the STMS Agreements.

5.2 **Enurement and Assignment.** This Guarantee is for the benefit of the Province and its permitted successors and assigns. This Guarantee will be binding upon and enure to the benefit of the Parties and their respective successors and permitted assigns. EDS Canada may not assign its obligations under this Guarantee or any part thereof without the prior written consent of the Province. The Province may assign this Guarantee and its benefits and interest therein in conjunction with the assignment of the interest of the Province in, to and under the STMS Agreements in accordance with their terms.

5.3 **Notice.** Wherever under this Guarantee EDS Canada or the Province is required or

permitted to give notice to, inform or advise the other, such notice shall be in writing and shall be delivered personally or sent by nationally recognized express courier. Any such notice shall be deemed given when actually received and shall be addressed as follows:

To the Province:

The Province of British Columbia
West 334 E 4000 Seymour Place
Victoria, British Columbia
V8W 9V1

Attn: Executive Director, Enterprise Hosting Solutions, Workplace Technology Services

To EDS Canada:

EDS Canada Inc.
33 Yonge St.
Suite 500
Toronto, Ontario
M5E 1G4

Attn: General Counsel

EDS Canada or the Province may change its address for notices upon giving prior written notice of the change to the other in the manner provided above.

5.4 **Amendments.** No modification, amendment or waiver of any of the provisions of this Guarantee shall be binding upon the Province unless expressly set forth in a writing signed on behalf of the Province, and then shall be effective only in the specific instance and for the purpose for which given.

5.5 **Waiver.** The observance of any term of this Guarantee may be waived by the Province, but such waiver shall be effective only if it is in writing and signed by the Province. No delay or omission on the part of the Province in exercising any right or privilege under this Guarantee shall operate as a waiver thereof, nor shall any waiver on the part of the Province of any right or privilege under this Guarantee operate as a waiver of any other right or privilege under this Guarantee nor shall any single or partial exercise of any right or privilege preclude any other or further exercise thereof or the exercise of any other right or privilege under this Guarantee. A waiver by the Province of any right or remedy on any occasion shall not be construed as a bar to any right or remedy that the Province would otherwise have on any future occasion.

5.6 **Further Assurances.** EDS Canada will, from time to time, execute and deliver all such further documents and instruments and do all such further acts and things as the Province may reasonably require to carry out or better evidence or perfect the full intent and meaning of this Guarantee.

5.7 **Costs.** In the event of any legal proceedings related to this Guarantee, the prevailing party shall be entitled to recover from the non-prevailing party reasonable legal fees and costs.

5.8 **Disputes.** Any dispute relating to this Guarantee shall be resolved in accordance with the dispute resolution procedures contained in the Agreement.

5.9 **Governing Law.** This Guarantee shall be governed by and construed in accordance with the laws, other than choice of law rules, of the Province of British Columbia and, to the extent applicable, the federal laws of Canada. The Parties hereby irrevocably submit to the exclusive jurisdiction of the courts of the Province of British Columbia and agree that any action which may be brought in connection with this Guarantee shall be brought in the Province of British Columbia.

5.10 **Language.** The parties have agreed that this Guarantee and all documents related thereto will be drafted in the English language. Les parties aux présentes ont convenu que cette convention et tous les documents qui s'y rapportent soient rédigés en langue anglaise.

5.11 **Counterparts.** This Guarantee may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one agreement binding on all the Parties, notwithstanding that all the Parties are not signatories to the original or same counterpart.

IN WITNESS WHEREOF, EDS Canada has caused this Guarantee to be executed and delivered by its duly authorized representative, as of the date and year first set forth above.

EDS CANADA INC.

By: _____

Name: _____

Title: _____

SCHEDULE 33

CORPORATE GUARANTEE

(Section 25.7)

CORPORATE GUARANTEE

This Guarantee is executed as of _____, by **HEWLETT-PACKARD COMPANY** ("**HP**"), a corporation incorporated under the laws of Delaware with an office at _____, for the benefit of **HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA** (the "**Province**"), **as represented by the Minister of Labour and Citizens' Services.**

WHEREAS, EDS Advanced Solutions Inc. ("**EDS Subsidiary**"), a British Columbia corporation with a place of business at Vancouver Island Technology Park, 2200-4464 Markham Road, Victoria, British Columbia, V8Z 7X8 and the Province concurrently herewith have executed a certain Master Services Agreement (the "**Agreement**") dated as of _____ (terms capitalized in this Guarantee but not defined in this Guarantee shall have the meanings given to them in the Agreement); and

WHEREAS, as a condition to entering into the Agreement, the Province has required that HP deliver this written Guarantee of certain obligations of EDS Subsidiary set forth in the Agreement and the Transaction Documents; and

NOW THEREFORE HP makes this Guarantee knowing that the Province shall rely on this Guarantee in entering into the STMS Agreements (defined below). HP conclusively acknowledges that reliance by the Province on this Guarantee is in every respect justifiable and that it received adequate and fair and valuable consideration for this Guarantee, the receipt and adequacy of which are hereby acknowledged. Subject to the terms and conditions hereof, HP hereby agrees as follows:

1. GUARANTEE AND UNDERTAKING

1.1 **Guaranteed Obligations.** For purposes of this Guarantee, "**Guaranteed Obligations**" means the payment of all debts and liabilities of EDS Subsidiary to the Province arising from EDS Subsidiary's performance of, or failure to perform, its obligations under, pursuant to, or in connection with the Agreement or any of the other Transaction Documents (collectively, the "**STMS Agreements**").

1.2 **Guarantee.** HP hereby absolutely, unconditionally and irrevocably guarantees to the Province the performance by EDS Subsidiary of the Guaranteed Obligations of EDS Subsidiary, all in accordance with and subject to the terms and conditions of this Guarantee. If EDS Subsidiary defaults in any material respect in the performance of any of the Guaranteed Obligations (other than for reasons which result in EDS Subsidiary being excused from performing such obligations), and fails to cure such default prior to the expiration of any applicable notice or cure period, then within a reasonable period of time following HP's receipt of written notice from the Province of EDS Subsidiary's default, HP shall cause to be performed the Guaranteed Obligations in accordance with the terms and conditions of the STMS Agreements, and at no cost to the Province other than as provided in the STMS Agreements.

2. CONTINUING NATURE OF GUARANTEE

2.1 **Continuing and Irrevocable.** This Guarantee shall be continuing and irrevocable until all of the Guaranteed Obligations have been fulfilled or otherwise satisfied, at which time this Guarantee shall automatically terminate and expire.

2.2 **Limitation of Liability.** The liability of HP under this Guarantee shall be coextensive with, but not in excess of, the liability of EDS Subsidiary to the Province under the STMS Agreements, and HP shall be entitled to the benefit of and may assert all rights, defenses, counterclaims, and other protections to which EDS Subsidiary may be entitled with respect to any such liability, including without limitation, all provisions of the STMS Agreements relating to the limitation of liability, limitation periods with respect to Claims under the STMS Agreements and the resolution of disputes. In no event shall the aggregate liability of HP, any other Affiliate of EDS Subsidiary who may have provided a guarantee of EDS Subsidiary's obligations and EDS Subsidiary under this Guarantee, any other such guarantee and the STMS Agreements exceed the liability of EDS Subsidiary under the STMS Agreements. Notwithstanding the foregoing, HP shall not be entitled to the benefit of the defenses, counterclaims and protections described in Section 2.3 below except to the extent that such defenses, counterclaims and protections are available to EDS Subsidiary.

2.3 **No Release.** The liability of HP under this Guarantee shall not be released, reduced, impaired or affected by or as a result of any matter or thing whatsoever that would otherwise release or discharge a guarantor or limit its obligations (except as set forth in Section 2.2 above), including any of the following:

(a) any withdrawal of any demand (including the commencement and continuance of any legal proceedings) by the Province for performance by HP of any Guaranteed Obligations under this Guarantee;

(b) if, whether or not with HP's knowledge, the Province grants extensions of time, renewals, indulgences, amendments, modifications, waivers, releases, discharges, makes any compromise or transaction or arrangement, or otherwise deals with any of the Guaranteed Obligations, the STMS Agreements, EDS Subsidiary, or with any security, guarantee or similar assurance held by it;

(c) any compromise by the Province of any of the Guaranteed Obligations or any other guarantee in respect thereof;

(d) the voluntary or involuntary liquidation, dissolution, consolidation or merger (or the sale or other disposition of all or part of the assets) of HP or EDS Subsidiary or any of their respective Affiliates;

(e) insolvency, bankruptcy, receivership, assignment for the benefit of creditors or reorganization, arrangement, composition or readjustment of debt, or other similar proceeding affecting HP, EDS Subsidiary or any of their respective Affiliates, or any similar proceedings instituted by or against HP, EDS Subsidiary or the assets of either of them; or

(f) the failure of the Province or any other party to take, protect or preserve any rights, security, guarantee or similar assurance of EDS Subsidiary or any other Affiliate of EDS Subsidiary (other than the rights and security of EDS Subsidiary and its Affiliates referred to in Schedule 23 of the Agreement, if any), whether or not caused or resulting

from any act or omission of the Province or any person acting for the Province or for whom the Province may be responsible.

3. PROCEEDINGS UNDER GUARANTEE

3.1 **Proceeding Against HP.** The Province shall not proceed against HP in respect of the Guaranteed Obligations until EDS Subsidiary shall have defaulted in a material respect in the performance of such Guaranteed Obligations (other than for reasons which result in EDS Subsidiary being excused from performing such obligations), and shall have failed to cure such default prior to the expiration of any applicable notice or cure period. The Province shall provide HP with a copy of any notice of default delivered by the Province to EDS Subsidiary at the same time as such notice of default is delivered by the Province to EDS Subsidiary. Any failure by the Province to pursue rights or remedies against any other guarantor shall not relieve HP from its obligations under this Guarantee.

3.2 **Reinstatement.** This Guarantee shall be reinstated if at any time any amounts paid on account of any Guaranteed Obligations must be returned by the Province upon the insolvency, bankruptcy, dissolution, liquidation or reorganization of the HP, EDS Subsidiary or any of their respective Affiliates.

3.3 **Set Off.** Any amounts owed to EDS Subsidiary by the Province under the Agreement or the Transaction Documents or otherwise in respect of the Services, but excluding any amounts under Dispute may be set-off by HP against the Guaranteed Obligations.

4. REPRESENTATIONS, WARRANTIES AND OTHER COVENANTS

4.1 **Representations.** HP represents and warrants as follows to the Province, as of the date of this Guarantee, and acknowledges and agrees that the Province is relying on such representations and warranties and is entitled to do so in entering into this Guarantee and the STMS Agreements:

(a) HP is a company duly incorporated and validly existing under the laws of Delaware and is in good standing under such laws;

(b) HP has all necessary power, capacity and legal authority to enter into, execute and deliver this Guarantee and to perform its obligations hereunder, and this Guarantee has been duly executed and delivered by HP, and constitutes a legal, valid and binding obligation of HP enforceable against HP in accordance with its terms, subject to applicable bankruptcy, insolvency and other laws of general application limiting the enforceability of creditors' rights, and to the fact that specific performance and injunctive relief are equitable remedies available only in the discretion of the court;

(c) neither the execution and delivery of this Guarantee, nor the compliance with the terms of this Guarantee by HP:

(i) has resulted or will result in a violation of any applicable laws;

(ii) has resulted or will result in a breach of, or constitute a default under, HP's constating documents, any shareholders' agreement to which it is a party or any shareholder or directors' resolutions, which would have a material adverse effect on HP's ability to perform its obligations under this Guarantee, or

(iii) has resulted or will result in a material breach of, or constitute a material default under any instrument or agreement to which HP is a party or by which HP is bound, which breach or default would have a material adverse effect on HP's ability to perform its obligations under this Guarantee.

4.2 **Taxes.** Any and all payments by HP to the Province under this Guarantee shall be made free and clear of and without deduction for any and all present or future taxes, levies, imposts, deductions, charges or withholdings, and all liabilities with respect thereto, excluding those that shall be adjusted for in accordance with this Section. If HP shall be required by law to deduct any such amounts from or in respect of any sum payable to the Province under this Guarantee, then:

(a) the sum payable shall be increased as may be necessary so that after making all required deductions (including deductions applicable to additional sums payable under this Section) the Province will receive an amount equal to the sum it would have received had no such deductions been made;

(b) HP shall make such deductions; and

(c) HP shall pay the full amount deducted to the relevant Governmental Authority in accordance with Applicable Laws.

5. MISCELLANEOUS

5.1 **STMS Agreements.** HP acknowledges that it is aware of the obligations of EDS Subsidiary under the STMS Agreements. HP expressly agrees that: (i) the Province is not required to provide HP with, and HP hereby waives any right to receive from the Province, copies of the STMS Agreements or any amendments to the STMS Agreements; and (ii) the obligations of HP to the Province under this Guarantee shall in no way be affected, diminished or otherwise limited as a result of any amendments made by EDS Subsidiary and the Province to the STMS Agreements.

5.2 **Enurement and Assignment.** This Guarantee is for the benefit of the Province and its permitted successors and assigns. This Guarantee will be binding upon and enure to the benefit of the Parties and their respective successors and permitted assigns. HP may not assign its obligations under this Guarantee or any part thereof without the prior written consent of the Province. The Province may assign this Guarantee and its benefits and interest therein in conjunction with the assignment of the interest of the Province in, to and under the STMS Agreements in accordance with their terms.

5.3 **Notice.** Wherever under this Guarantee HP or the Province is required or permitted to give notice to, inform or advise the other, such notice shall be in writing and shall be delivered personally or sent by nationally recognized express courier. Any such notice shall be deemed given when actually received and shall be addressed as follows:

To the Province:

The Province of British Columbia
West 334 E 4000 Seymour Place
Victoria, British Columbia
V8W 9V1

Attn: Executive Director, Enterprise Hosting Solutions, Workplace Technology Services

To HP:

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, California
94304

Attn: _____

HP or the Province may change its address for notices upon giving prior written notice of the change to the other in the manner provided above.

5.4 **Amendments**. No modification, amendment or waiver of any of the provisions of this Guarantee shall be binding upon the Province unless expressly set forth in a writing signed on behalf of the Province, and then shall be effective only in the specific instance and for the purpose for which given.

5.5 **Waiver**. The observance of any term of this Guarantee may be waived by the Province, but such waiver shall be effective only if it is in writing and signed by the Province. No delay or omission on the part of the Province in exercising any right or privilege under this Guarantee shall operate as a waiver thereof, nor shall any waiver on the part of the Province of any right or privilege under this Guarantee operate as a waiver of any other right or privilege under this Guarantee nor shall any single or partial exercise of any right or privilege preclude any other or further exercise thereof or the exercise of any other right or privilege under this Guarantee. A waiver by the Province of any right or remedy on any occasion shall not be construed as a bar to any right or remedy that the Province would otherwise have on any future occasion.

5.6 **Further Assurances**. HP will, from time to time, execute and deliver all such further documents and instruments and do all such further acts and things as the Province may reasonably require to carry out or better evidence or perfect the full intent and meaning of this Guarantee.

5.7 **Costs**. In the event of any legal proceedings related to this Guarantee, the prevailing party shall be entitled to recover from the non-prevailing party reasonable legal fees and costs.

5.8 **Disputes**. Any dispute relating to this Guarantee shall be resolved in accordance with the dispute resolution procedures contained in the Agreement.

5.9 **Governing Law**. This Guarantee shall be governed by and construed in accordance with the laws, other than choice of law rules, of the Province of British Columbia and, to the extent applicable, the federal laws of Canada. The Parties hereby irrevocably submit to the exclusive jurisdiction of the courts of the Province of British Columbia and agree that any action which may be brought in connection with this Guarantee shall be brought in the Province of British Columbia.

5.10 **Language**. The parties have agreed that this Guarantee and all documents related thereto will be drafted in the English language. Les parties aux présentes ont convenu que cette convention et tous les documents qui s'y rapportent soient rédigés en langue anglaise.

5.11 **Counterparts**. This Guarantee may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one agreement binding on all the Parties, notwithstanding that all the Parties are not signatories to the original or same counterpart.

IN WITNESS WHEREOF, HP has caused this Guarantee to be executed and delivered by its duly authorized representative, as of the date and year first set forth above.

HEWLETT-PACKARD COMPANY

By: _____

Name: _____

Title: _____

SCHEDULE 34

INSURANCE

(Article 26)

1. **Commercial General Liability.** Commercial general liability insurance protecting against damage from personal injury (including death) and from claims for property damage that may arise out of the operations of the Service Provider and its employees under this Agreement. Such insurance shall be for an amount of not less than ten million dollars ($10,000,000) inclusive for any one occurrence and may be provided by way of a combination of policies including primary policies, umbrella or excess policies. Such policy or policies shall be on an occurrence basis and shall provide coverage for bodily injury and property damage, non-owned automobile liability, personal injury liability, employer's liability, blanket contractual liability coverage, broad form property damage coverage and coverage for products and completed operations. The policy shall contain a cross-liability clause, and shall name the Province as an additional insured.

2. **Errors & Omissions Liability.** The Services Provider shall maintain errors and omissions liability insurance covering liability for claims arising out of an error, omission by the Service Provider in the performance or provision of the Services in an amount per occurrence and in the aggregate of not less tha

BRITISH COLUMBIA
The Best Place on Earth

CERTIFICATE OF INSURANCE

Freedom of Information and Protection of Privacy Act
The personal information requested on this form is collected under the authority of and used for the purpose of administering the *Financial Administration Act*. Questions about the collection and use of this information can be directed to the Director, Client Services, Core Government and Crowns at 250 356-8915, PO Box 9405 Stn Prov Govt, Victoria BC V8W 9V1.
Please refer *all other questions* to the contact named in Part 1.

Part 1 – To be completed by the Province

THIS CERTIFICATE IS REQUESTED BY AND ISSUED TO *(Name of office)*	AGREEMENT IDENTIFICATION NO.

PROVINCE'S CONTACT PERSON

NAME	TITLE	PHONE NO.	FAX NO.
		( )	( )

MAILING ADDRESS	POSTAL CODE

CONTRACTOR NAME

CONTRACTOR ADDRESS	POSTAL CODE

Part 2 – To be completed by Insurance Agent or Broker

INSURED	NAME	
	ADDRESS	POSTAL CODE
OPERATIONS INSURED	PROVIDE DETAILS	

TYPE OF INSURANCE (List each separately)	COMPANY NAME, POLICY NO. AND BRIEF DESCRIPTION	EXPIRY DATE YYYY / MM / DD	LIMIT OF LIABILITY/AMOUNT

This certificate certifies that policies of insurance described herein are in full force and effective as of the date of this certificate and comply with the insurance requirements of the Agreement identified above, except as follows:

AGENT OR BROKER COMMENTS

AGENT OR BROKER	ADDRESS – *include postal code*	PHONE NO.
		( )

SIGNED BY THE AGENT OR BROKER ON BEHALF OF THE ABOVE INSURER(S)	DATE SIGNED YYYY MM DD
X	

SCHEDULE 36

MATERIAL BREACH

(Section 28.1)

NIL

SCHEDULE 37

At issue for Inquiry

Page 1702 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
At issue for Inquiry

SCHEDULE 38

TERMINATION FEES

1. The purpose of this Schedule 38 (*Termination Fees*) is to set forth the Parties agreement with respect to the allocation of specific costs of the Parties under the following circumstances:
   (a) the expiry of the Agreement ("Column 3" of the Termination Fees Allocation Matrix below);

   (b) termination of the Agreement by the Service Provider for Province Material Breach ("Column 4" of the Termination Fees Allocation Matrix below);

   (c) termination of the Agreement by the Province for convenience (Column 4 of the Termination Fees Allocation Matrix below); and

   (d) termination of the Agreement by the Province for the Service Provider Material Breach ("Column 5" of the Termination Fees Allocation Matrix below).

2. The Termination Fees Matrix summarizes the costs payable by each Party in the event of: (a) early termination of the Agreement, depending upon the circumstances of such termination; or (b) expiry of the Agreement. The Parties hereby agree to adopt and adhere to the following principles in connection with the Termination Fees Allocation Matrix:
   (a) the cost categories in each of the rows under "Column 2" of the Termination Fee Allocation Matrix are (1) calculated as the aggregate amount applicable to all SOWs in effect under the Agreement at the time of expiry or earlier termination of the Agreement; and (2) are without duplication, taking into account the costs addressed in any BPS Services Agreement in effect at the time of expiry or early termination;

   (b) in accordance with the Agreement and upon the expiry or earlier termination of the Agreement, the Parties will use commercially reasonable efforts to work cooperatively to mitigate the costs incurred by each Party as a result of such expiry or earlier termination;

   (c) unless the Parties agree otherwise and subject to Article 19 (*Intellectual Property and Proprietary Rights*) and Schedule 43 (*Software Responsibility Table*), any third party contracts (including, without limitation, software license agreements, software maintenance agreements, lease agreements and any other agreements with third parties) entered into by the Service Provider in connection with the provision of the Services by the Service Provider to the Province will include the right to assign or otherwise transfer such third party contracts to the Province or its Alternate Service Provider at no cost other than commercially reasonable assignment or transfer administrative fees

(d) upon early termination or expiry of the Agreement, for each of the cost categories in each of the rows under "Column 2" of the Termination Fees Allocation Matrix, each Party, as the case may be, will provide documentary evidence of the costs that are to be paid by the other Party (as applicable);

(e) where the Province is entitled or obligated under the Termination Fees Allocation Matrix to take assignment of contracts or to acquire certain assets or employees, the Province may assign such entitlements or obligations to its Alternate Service Provider

(f) in the event that the Service Provider enters into other BPS Services Agreements with Broader Public Sector entities after the Effective Date, this Schedule will be updated to address the Relocation Costs of the Broader Public Sector entities in the case of a termination for convenience by the Province. The Parties will add a new row into the cost category 11.0 (Broader Public Sector Relocation Costs).; and

(g) in the event that a BPS Customer terminates its BPS Services Agreement for Service Provider Material Breach, or for convenience , or if the Service Provider terminated the BPS Services Agreement for BPS Customer Default, the Parties will reduce the Province VA Commitment, as more particularly described in Appendix E.

Termination Fee Allocation Matrix

	Column 2	Column 3	Column 4	Column 5
Row #	Cost Item *Definitions/comments*	Expiry of Agreement	Termination by Service Provider for Province Material Breach or Termination by Province for Convenience	Termination by Province for Service Provider Material Breach
1.0	TRANSFORMATION COSTS			
1.1	Transformation Projects	N/A	Province will pay the Service Provider the transformation costs, including the transformation financing costs, incurred to date by the Service Provider up to the termination date.	The Province will pay the Service Provider any unpaid fees, including the transformation financing costs incurred to date, for the transformation deliverables completed up to the termination date. All other costs shall be the responsibility of the Service Provider.
1.2	Other transformation investments and financing costs (the transformation investment is not duplicative of the transformation financing costs associated with the Transformation Projects in row 1.1) (See Appendix A)	N/A	For the month in which the early termination occurs, the Province shall pay the Service Provider the amount set forth in Appendix A for the month in which termination occurs if such monthly amount is greater than zero. If such monthly amount is less than zero, the Service Provider shall pay the Province such amount as set forth in Appendix A.	For the month in which the early termination occurs, the Province shall pay the Service Provider the amount set forth in Appendix A for the month in which termination occurs if such monthly amount is greater than zero. If such monthly amount is less than zero, the Service Provider shall pay the Province such amount as set forth in Appendix A.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
2.0	**DEDICATED HARDWARE** *"Redeployment Costs" are the labour costs to de-install and re-install hardware* *"**Transfer Costs**" are the costs to transfer any hardware maintenance/support agreements.*			

Row #	Column 2 Cost Item *Definitions/comments*	Column 3 Expiry of Agreement	Column 4 Termination by Service Provider for Province Material Breach or Termination by Province for Convenience	Column 5 Termination by Province for Service Provider Material Breach
2.1	Dedicated hardware part of third party financing by Service Provider *"**Dedicated Hardware**" means any hardware that is used by the Service Provider 50% or more for the purpose of performing the Services under the Agreement.*	Province's option to: (i) take assignment of lease and continue to make lease payments to the third party financier; or (ii) acquire the Dedicated Hardware by paying the Service Provider the present value of the remaining payments using a 5% discount rate. Province is responsible for Service Provider's costs associated with the Dedicated Hardware Redeployment and Transfer Costs, at the Standard Time and Materials Rates as set forth in Schedule 23 (*Fees*).	Province will acquire the Dedicated Hardware by paying the Service Provider the present value of the remaining payments using a 5% discount rate. Province is responsible for Service Provider's costs associated with the Dedicated Hardware Redeployment and Transfer Costs, at the Standard Time and Materials Rates as set forth in Schedule 23 (*Fees*).	Province's option to: (i) take assignment of lease and continue to make lease payments to the third party financier; or (ii) acquire the Dedicated Hardware by paying the Service Provider the present value of the remaining payments using a 5% discount rate; or (iii) costs of the Dedicated Hardware remains the Service Provider's responsibility. If Province exercises the option to acquire Dedicated Hardware under (i) or (ii) above, then the Service Provider is responsible for costs associated with hardware Redeployment and Transfer Costs.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
2.2	Province funded hardware, part of the Capital Payment ("**Funded Hardware**")	Ownership of the Funded Hardware transfers to the Province free and clear of any Liens and subject to the provisions in Section 15.5 (*Right of Set-Off*). Province is responsible for Service Provider's costs associated with hardware Redeployment Costs and Transfer Costs, at the Standard Time and Materials Rates as set forth in Schedule 23 (*Fees*).	Ownership of the Funded Hardware transfers to the Province free and clear of any Liens and subject to the provisions in Section 15.5 (*Right of Set-Off*). Province is responsible for Service Provider's hardware Redeployment Costs and Transfer Costs, at the Standard Time and Materials Rates as set forth in Schedule 23 (*Fees*).	Ownership of the Funded Hardware transfers to the Province free and clear of any Liens and subject to the provisions in Section 15.5 (*Right of Set-Off*). Service Provider is responsible for hardware Redeployment Costs and Transfer Costs.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
2.3	Dedicated hardware not part of third party financing by Service Provider or Province Funded Hardware	Province's option to acquire hardware by paying the Service Provider a negotiated price; otherwise Service Provider responsibility. If Province exercises option to acquire hardware then Province responsible for Service Provider's Redeployment Costs and Transfer Costs, at the Standard Time and Materials Rates as set forth in Schedule 23(*Fees*).	Province will acquire hardware by paying the Service Provider's net book value. Province is responsible for Service Provider's hardware Redeployment Costs and Transfer Costs, at the Standard Time and Materials Rates as set forth in Schedule 23 (*Fees*).	Province's option to acquire hardware by paying the Service Provider a negotiated price; otherwise Service Provider responsibility. If Province exercises option to acquire hardware then the Service Provider is responsible for hardware Redeployment Costs and Transfer Costs.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
3.0	**SHARED ASSETS**			
3.1	Assets purchased by the Service Provider but not dedicated to the Province	Service Provider responsibility.	Province pays the Service Provider: i) The asset net book value multiplied by the percentage of the asset used for delivering the Services; ii) The value of remaining lease payments multiplied by the percentage of the asset used for delivering the Services. The Service Provider retains ownership.	Service Provider responsibility.
4.0	**SOFTWARE COSTS**			
4.1	Software Costs	As per Article 19 (*Intellectual Property and Proprietary Rights*) and Schedule 43 (*Software Responsibility Table*).	As per Article 19 (*Intellectual Property and Proprietary Rights*) and Schedule 43 (*Software Responsibility Table*).	As per Article 19 (*Intellectual Property and Proprietary Rights*) and Schedule 43 (*Software Responsibility Table*).
5.0	**FACILITIES COSTS**			
5.1	Facilities excluding the STMS Data Centres	Service Provider responsibility.	Province pays the Service Provider: i) The remaining value of the lease payments; ii) The net book value of the leasehold improvements and furniture.	Service Provider responsibility.

	Column 2	Column 3	Column 4	Column 5
Row #	Cost Item *Definitions/comments*	Expiry of Agreement	Termination by Service Provider for Province Material Breach or Termination by Province for Convenience	Termination by Province for Service Provider Material Breach
5.2	STMS Data Centres	N/A	The Province shall pay the STMS Data Centre Termination Fees to the Service Provider as set forth in Appendix B and in accordance with the provisions of Appendix C.	Refer to Schedule 5 , Section 29
6.0	**OTHER THIRD PARTY CONTRACTS**			
6.1	Material Subcontractors excluding Data Centre Subcontractor	Service Provider responsibility	Province option to take assignment of the subcontract. Province pays the cancellation and transfer costs per subcontract provided they are disclosed in writing to the Province at the time the subcontract was entered into by the Service Provider.	Province option to take an assignment of the subcontract. Service Provider pays cancellation or transfer costs.
6.2	Other third party contracts (other than software licenses and facilities)	Province option to take an assignment of third party. If Province exercises option to take assignment of third party contract then the Province is responsible for assignment costs.	If Service Provider requires Province to take assignment of third party contracts then Province responsible for on-going costs If Service Provider requires Province to take assignment of third party contracts then the Province is responsible for assignment costs.	Province option to take an assignment of third party contract and Province responsible for on-ongoing costs. If Province exercises option to take assignment of third party contract then the Province is responsible for assignment costs.

	Column 2	Column 3	Column 4	Column 5
Row #	Cost Item *Definitions/comments*	Expiry of Agreement	Termination by Service Provider for Province Material Breach or Termination by Province for Convenience	Termination by Province for Service Provider Material Breach
7.0	**EMPLOYEE COSTS**			
7.1	EDS Advanced Solutions and EDS Canada Employee Costs *"**Available Personnel**" are employees spending 75% or greater of their work time on providing the Services. The 75% is based on the final 6 months before expiry or early termination of the Agreement, as applicable.*	Province option to offer employment to Available Personnel. For Available Personnel who (i) do not receive an offer, or (ii) received an offer but get bumped under the Collective Agreement by more senior Available Personnel; the Province will reimburse Service Provider for the severance cost of the Available Personnel. The Service Provider will attempt to redeploy Available Personnel within EDS Canada or EDS Advanced Solutions as appropriate from a labour relations perspective.	Province option to offer employment to Available Personnel. For Available Personnel who (i) do not receive an offer, or (ii) received an offer but get bumped under the Collective Agreement by more senior Available Personnel; the Province will reimburse Service Provider for the severance cost of the Available Personnel. The Service Provider will attempt to redeploy Available Personnel within EDS Canada or EDS Advanced Solutions as appropriate from a labour relations perspective.	Province option to offer employment to Available Personnel. For Available Personnel who (i) do not receive an offer, or (ii) received an offer but get bumped under the Collective Agreement by more senior Available Personnel; the Province will reimburse Service Provider for the related severance cost of the Available Personnel. The Service Provider will attempt to redeploy Available Personnel within EDS Canada or EDS Advanced Solutions as appropriate from a labour relations perspective. Service Provider is responsible for all severance costs for any Available Personnel that refuse the offer.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
8.0	**PREPAID EXPENSES**			
8.1	Prepaid Expenses	Where the Province exercises its option to acquire hardware or take an assignment of contracts, the Province will pay the Service Provider the remaining balance of prepaid expenses related to the acquired hardware and contracts.	For hardware acquired or contracts assigned to the Province, the Province will pay the Service Provider the remaining balance of prepaid expenses related to the acquired hardware and assigned contracts.	Where the Province exercises its option to acquire hardware or take an assignment of contracts, the Province will pay the Service Provider the remaining balance of prepaid expenses related to the acquired hardware and contracts.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
9.0	**STMS DATA CENTRE RELOCATION COSTS**			
9.1	STMS Data Centre Relocation Costs (as defined in Appendix D)	The Province shall be responsible for any and all Relocation Costs incurred by the Province.	Province shall be responsible for any and all Relocation Costs incurred by the Province.	Service Provider shall be responsible for and shall reimburse the Province for the Relocation Costs incurred by the Province, subject to the provisions of Schedule 31 (*Limitation on Liability*) which for all purposes under this Agreement shall be considered Direct Damages.
10.0	**TERMINATION SERVICES**			
10.1	Termination Services	Termination Services will be provided by the Service Provider in accordance with Article 29 (*Termination Services*) of the Agreement.	Termination Services will be provided by the Service Provider in accordance with Article 29 (*Termination Services*) of the Agreement.	Termination Services will be provided by the Service Provider in accordance with Article 29 (*Termination Services*) of the Agreement.

	Column 2	Column 3	Column 4	Column 5
Row #	**Cost Item** *Definitions/comments*	**Expiry of Agreement**	**Termination by Service Provider for Province Material Breach or** **Termination by Province for Convenience**	**Termination by Province for Service Provider Material Breach**
11.0	**BROADER PUBLIC SECTOR**			
11.1	ICBC Capacity Reservation	N/A	Province shall be responsible for any and all Termination for Convenience Fees incurred by ICBC's Capacity Reservation.	Refer to BPS Services Agreement.

Note 1: The Province will vacate its Customer Environment at the STMS Data Centres by the last day of a calendar month (the "**Exit Date**"), and will continue to pay for the Province VA Commitment or Adjusted Province VA Commitment, until the Exit Date.

APPENDIX A
TRANSFORMATION INVESTMENTS AND FINANCING COSTS

The following is in reference to row 1.2 of the Termination Fee Matrix

APPENDIX B

STMS DATA CENTRE TERMINATION FEES
TERMINATION BY PROVINCE FOR CONVENIENCE
AND
TERMINATION BY SERVICE PROVIDER FOR PROVINCE MATERIAL BREACH

1 Table 1 below sets forth the STMS Data Centre termination fees payable by the Province to the Service Provider in the event of the following:

a. the Province elects to terminate the Agreement for its convenience pursuant to Section 28.5 (*Termination by Province for Convenience*) of the Agreement; or

b. the Service Provider terminates the Agreement for Province Material Breach pursuant to Section 28.3 (*Material Breach by Province*),

(the "**STMS Data Centre Termination Fee**").

The remaining fees that would have been payable by the Province to the Service Provider from the Exit Date to the end of the Term based on the Province VA Commitment at each STMS Data Centre is referred to as the "**Remaining Contract Value**". Accordingly, each STMS Data Centre has its own Remaining Contract Value.

2 The Province STMS Data Centre Termination Fees shown in Table 1 are based the following:

(a) The Agreement has been terminated and the Province has vacated the STMS Data Centres by the first day of the contract month ;

(b)

(c) Province VA Commitment of 1,200,000 VAs at STMS Interior Data Center and 300,000 VAs at STMS Calgary Data Centre;

(d) The Province VA Commitment is phased-in over 5 years as described in Schedule 23, Section 4.7 (*Phase-in of Province VA Commitment*);

(e)

3 As a result of conditions (b) to (d) above, the Parties will make the following adjustments to the Province STMS Data Centre Termination Fees :

(a) if the Province VA Commitment or the Province Adjusted VA Commitment is other than as described in Subsection (c) above, then the Remaining Contract Value will be adjusted accordingly;

(b) if the phase-in of the Province VA Commitment is other than as described in Subsection (d) above, then the Remaining Contract Value will be adjusted accordingly; and,

(c) if the VA Unit Price for either STMS Data Centre is other than as described in Subsection (b) above, then the Remaining Contract Value will be adjusted using the actual VA Unit Price in effect on the Exit Date (for example, to reflect Data Centre CPI adjustments and changes to the VA Unit Price for Province Adjusted VA Commitment);

4. The Service Provider will invoice the Province for the STMS Data Centre Termination Fee at least 10 Business Days prior to the Exit Date, and the Province will pay such invoice in accordance with the payment provisions of the Agreement.

5. The Service Provider will pay a Termination Fee Repayment to the Province in accordance with the circumstances more particularly described in Appendix C Termination Fee Repayment, to the extent applicable.

Pages 1719 through 1724 redacted for the following reasons:
- -
At issue for Inquiry

APPENDIX C
TERMINATION FEE REPAYMENT
STMS Interior Data Centre Termination Fee Repayment

1. The "**Termination Fee Repayment**" is an annual payment from the Service Provider to the Province that refunds part of the Province Termination Fees as a result of the Service Provider contracting the terminated VAs with a third party, in respect of the STMS Interior Data Centre.

   The Province VA Commitment or Province Adjusted VA Commitment for the STMS Interior Data Centre at the time of termination is referred to as the "**Terminated VAs**".

   The Service Provider will contract the Terminated VAs once all other VA capacity at the STMS Interior Data Centre is contracted to a third party (i.e., the Terminated VAs will be the last VAs contracted to a third party).

Annual Termination Fee Repayment Calculation

2. The Service Provider will calculate an annual Termination Fee Repayment based upon the following:
   (a) the number of Terminated VAs that the Service Provider has contracted with a third party;

   (b) multiplied by the VA Unit Price as of the Exit Date;

   (c) multiplied by the Termination Percentage; and

   (d) multiplied by the number of months for which the Terminated VAs were invoiced in the preceding calendar year to a third party.

3. The annual Termination Fee Repayment will be paid by the Service Provider to the Province in April each year for the preceding calendar year, where applicable.

4. If the Service Provider does not receive a VA price for the contracted VAs with the third party that is greater than or equal to the VA Unit Price as of the Exit Date, then the annual Termination Fee Repayment will be reduced to reflect the lower VA price as illustrated in the example below:

5. The Service Provider will assume all costs associated with the marketing and contracting for the Terminated VAs to a third party.

Terminated VAs Report

6. For the period commencing on the Exit Date to the expiry of the Initial Term DC Services, the Service Provider will produce an annual report for the period of January to December of each year indicating:
   (a) the STMS Interior Data Centre's VA capacity; and,
   (b) the actual contracted VA's to a third party.

   The Service Provider will provide the annual report to the Province by February 28th of each year.

STMS Calgary Data Centre Termination Fee Repayment

7. There is no Termination Fee Repayment for the STMS Calgary Data Centre.

Survival Clause

8. This Appendix survives the termination of the Agreement for the balance of the Initial Term DC Services, and for clarity, shall include any additional period or time as necessary to include a payment of the Termination Fee Repayment owing in respect of the last Contract Year of the Initial Term DC Services.

APPENDIX D

STMS DATA CENTRE RELOCATION COSTS

This Appendix describes the STMS Data Centre Relocation Costs that the Service Provider will pay to the Province on termination of the Agreement by the Province for a Service Provider Material Breach, subject to the provisions of Schedule 31 (*Limitation on Liability*) of the Agreement. The STMS Data Centre Relocation Costs include, but are not limited to, the following:

(a) Planning Costs - costs incurred by the Province associated with planning for the move out of the STMS Data Centres;

(b) Physical Costs - costs incurred by the Province associated with the physical move of equipment (such as servers, the mainframe and storage equipment) from the STMS Data Centres to temporary data centre space ("**Swing Space**") or new data centre(s);

(c) Swing Space Costs - costs incurred by the Province associated with Swing Space;

(d) Network Costs - costs incurred by the Province for the disconnection and reconnection of the network to the Swing Space and new data centre(s);

(e) System Testing - costs incurred by the Province associated with system regression and user acceptance testing; and

(f) BCP/DR – costs incurred by the Province associated with validating disaster recovery and business continuity plans in the new data centre.

APPENDIX E

CHANGES TO PROVINCE VA COMMITMENT DUE TO: TERMINATION BY BPS CUSTOMER FOR SERVICE PROVIDER MATERIAL BREACH, TERMINATION BY BPS CUSTOMER FOR CONVENIENCE OR TERMINATION BY SERVICE PROVIDER FOR DEFAULT BY BPS CUSTOMER

1. The purpose of this Appendix is to set forth the Parties agreement with respect to the treatment of the Province VA Commitment when the Agreement continues in force and is not terminated in the following circumstances:
    (a) termination of a BPS Services Agreement by a BPS Customer for Service Provider Material Breach;
    (b) termination of a BPS Services Agreement by a BPS Customer for convenience; or,
    (c) termination of a BPS Services Agreement by a Service Provider for default by the BPS Customer.
2. In each circumstance as set forth above, the BPS Customer and Service Provider will comply with the provisions of Schedule 38 (*Termination Fees*) of the BPS Services Agreement;
3. In the circumstances described in section (a) to (c) above, the Province may:
    (a) assumes responsibility for the BPS Customer's Capacity Reservation or Adjusted Capacity Reservation in each STMS Data Centre, and through a Change Order the monthly VAs Fees to the Province will increase by the corresponding amount of VAs represented by the BPS Customer's Capacity Reservation or Adjusted Capacity Reservation, as applicable. However, notwithstanding the forgoing, the Province VA Commitment will remain unchanged;
    (b) not assume responsibility for the Capacity Reservation or Adjusted Capacity Reservation of the BPS Customer, then the Province VA Commitment will be reduced by the quantity of the VAs terminated by the BPS Customer. The Province and remaining BPS Customers will continue to pay the same VA Unit Price for the remaining Province VA Commitment as the Province and remaining BPS Customer were paying prior to the termination of the BPS Services Agreement as set forth in section 1(a) to (c) above. For greater clarification, even if the termination of the BPS Service Agreement reduces the Province VA Commitment below the current volume band, the VA Unit Price will not increase as per the VA Price Table in Schedule 23 (*Fees*). For example:
        - The Province VA Commitment is 1,200,000 VAs for the STMS Interior Data Centre at a VA Unit Price of VA. At issue for Inquiry
        - The BPS Customer's Capacity Reservation is 200,000 VAs of the Province VA Commitment and the Province is paying for 1,000,000 VAs and the BPS Customer is paying for 200,000 VAs.
        - In the case of a termination of the BPS Customer's 200,000 VAs, the Province VA Commitment will be reduced by 200,000 VAs thereby changing from 1,200,000 VAs to 1,000,000 VAs.

- The Province will continue to pay the monthly VA Fees for 1,000,000 VAs at / VA

4. Where there has been a decrease to the Province VA Commitment as contemplated in Section 3 above, then the Province will not be entitled to a VA Unit Price reduction for any Province Additional VA Commitment as per Section 4 of Schedule 23 (*Fees*), until the Province VA Commitment is increased back to the Province VA Commitment at the applicable STMS Data Centres that was in place prior to the BPS Customer's termination of the BPS Services Agreement. To continue the example from above:

    - Since the Interior STMS Data Centre had an Province VA Commitment prior to the BPS Services Agreement termination of 1,200,000 VAs
    - the example above reduced the Province VA Commitment by 200,000 VAs to 1,000,000 VAs, the Province must increase the Province VA Commitment back to the original 1,200,000 VAs through a Province Additional VA Commitment, and then further increase the Province VA Commitment as described in the VA Price Table of Schedule 23 (*Fees*) in order to receive the lower VA Unit Price associated with the Province Additional VA Commitment.

SCHEDULE 39

SERVICE PROVIDER CODE OF CONDUCT

See the attached

ACTING WITH INTEGRITY

2008 EDS CODE OF BUSINESS CONDUCT

/// eds.com

EDS

Message From Ron Rittenmeyer

To the EDS Worldwide Team:

Everyone at EDS without exception has a responsibility to ensure we conduct every aspect of our business in the highest ethical standards and in compliance with legal requirements. This is simply good common sense in a global business environment. The EDS Code of Business Conduct is designed to help us meet this responsibility. While our business may require us to take reasonable and thoughtful operational risks, we must never compromise our ethical standards or legal responsibilities in executing our roles internally or externally.

The policy we follow without exception requires everyone to review the Code annually. This review is to remind everyone of our corporate standards and to ensure awareness and understanding of recent updates. The Code applies globally to all employees regardless of country, industry, client or situation. Our decisions every day at work must be consistent with the corporate standards set out in the Code.

Please make reviewing the Code a priority. In business, there can be nothing but absolute compliance with our corporate standards. Remember, our clients, shareholders and colleagues expect us to act ethically and in compliance with the law.

Thank you.

Ron Rittenmeyer
Chairman, President & Chief Executive Officer

Contents

Purpose of the EDS Code of Business Conduct (Code)

Doing business with integrity means that we act appropriately and play by the rules – both the laws and regulations that apply to us and the standards that we set for ourselves in company policies and this Code. Integrity helps us create successful long-term relationships and open communication with clients, fosters a strong sense of the corporate "family" and provides a better overall work environment.

Our Code is not – and is not intended to be – a rule book; instead, it is a guide to our corporate standards that applies globally to help all members of EDS' family do business with integrity. The Code is applicable to all the men and women employed by EDS and its subsidiaries, based on local law. Our directors are also subject to the Code, as applicable.

Each of us is responsible for putting the Code to work, but we do not have to go it alone. The company has a number of resources and people in place to answer our questions and guide us through difficult decisions. WHEN IN DOUBT, ASK!

Q: ***I'm getting ready to authorize a payment on behalf of EDS, which I think involves an "ethics" issue. Can you provide me with some guidance on how to analyze this issue?***

A: ***Life and business are complicated, and not all decisions are clearly right or wrong. When faced with a decision-making dilemma, apply the Ethics Quick Test and ask yourself:***

- ***Is the action legal?***
- ***How would it look in the newspaper?***
- ***Does it comply with EDS values and policies?***
- ***Am I treating others the same way I would choose to be treated?***
- ***If I do it, will I feel bad?***

If you're still uncertain about the best course of action, consult your leader or the Office of Ethics and Compliance.

Consulting Resources/Ethics Helpline

The Ethics Helpline: It is Accessible, Immediate and, if you choose, Anonymous.

If you have a question or concern, your leader or your leader's leader is an excellent resource. If you prefer, you can exercise the Open Door Policy, which allows you to talk to any leader in the company about any work-related issue without fear of retribution. Additionally, you can raise your work-related issues with Human Resources, Legal Affairs, or with the Office of Ethics and Compliance. The Office of Ethics and Compliance can offer you guidance on the content of the Code as well as EDS' policies and business practices.

At times you may want confidential advice about a business ethics dilemma. You can speak with a member of EDS' Office of Ethics and Compliance by calling 972 605 5607 or 972 605 5564. You may also contact the Office of Ethics and Compliance through use of the Ethics Inquiry electronic message function on the Ethics and Compliance Web page. All calls and Ethics Inquiry electronic messages will be treated confidentially to the extent reasonably possible. EDS prohibits retaliation in any form against employees for seeking advice or for making good faith reports of suspected misconduct.

You may also contact the Office of Ethics and Compliance through use of the Ethics Helpline by calling toll-free 1 888 337 3845 (888 EDS ETHK) if you are in the U.S. or Canada. Callers from other countries can dial toll-free by entering their country's access number + 888 337 3845. Click here to view country access codes. Helpline staff is available 24 hours a day, every day, and language translation services are available.

Although you are encouraged to identify yourself, you may remain anonymous when calling the Ethics Helpline or when using the Ethics Inquiry electronic message function. Local laws may limit the use of anonymous reporting to specific types of matters, and EDS processes incorporate these limits. Whether you identify yourself or not, all inquiries and discussions will be kept confidential to the extent reasonably possible. Your name will be used only on a "need-to-know" basis.

EDS' Corporate Policies discuss many of the laws and regulations that govern our business, and may assist you in determining the best course of conduct in a given situation. Please visit http://infocentre.eds.com/workplace/corp_policies to access those policies.

Q: ***When I call the Ethics Helpline, who is on the other end of the phone?***

A: ***EDS has contracted with an outside company to run the Ethics Helpline for us. This company has a staff of professionals who have been trained to listen and appropriately document your questions and reports. These professionals may ask you questions to gather more information. You will be given a report number and specific date to call back to get a response to your question or to check the status of your report. The outside company then sends information about your matter to the Office of Ethics and Compliance for action.***

Q: ***When I call the Ethics Helpline, is it really confidential?***

A: ***Questions and suspected misconduct reported to the Ethics Helpline are kept confidential to the extent reasonably possible, given EDS' need to answer your question or to conduct an investigation and appropriately resolve any issues. Investigations of suspected misconduct may involve asking questions of your colleagues or others, where information is sometimes disclosed. You can be assured, though, that the company will disclose information only on a need-to-know basis. And you should remember the company's over-arching commitment to prohibit retaliation in any form.***

Reporting Concerns

If you know of or suspect a violation of EDS policy or the law, you **must** report it to your leader, Legal Affairs, the Office of Ethics and Compliance, or the Ethics Helpline. EDS strictly prohibits discrimination or retaliation in any form against employees for making good faith reports.

You can harm EDS not only by acting inappropriately, but also by NOT acting when it is your responsibility to do so. If you suspect misconduct, it is your obligation to report it.

Q: ***We just finalized and signed a three-year contract with a big new client, and it means a lot to our team. The contract that we signed states that the work will begin in four months, after the client's fiscal year ends, but there is a side letter that clarifies that the work is actually to begin immediately. I suspect that the contract is drafted that way so that the client doesn't have to report any expenses related to the contract in this fiscal year. I know the deal was reviewed and approved by senior management, so I don't think I need to report this to anyone. Besides, the reporting issue really is an issue for the client, and not EDS. Is that correct?***

A: ***No, it is not. Any time that you suspect misconduct, you must report it. It may be that senior management approved the deal without knowledge of the side letter. If you suspect senior management knew about the side letter and nevertheless approved the deal without inquiring into the appropriateness of the arrangement under applicable laws, you must report it. And if you're uncertain about whether a particular arrangement is improper, or whether senior management had knowledge of certain information, it is your obligation to ask appropriate personnel. EDS' commitment to acting with integrity means that we do not knowingly assist a client, supplier or anyone else in violating or avoiding legal obligations, including disclosure obligations under the securities laws.***

If you don't feel comfortable talking to your leader about the issue (because he or she already knows of and has approved the conduct in question), then you should talk to Legal Affairs, the Office of Ethics and Compliance, or the Ethics Helpline. Remember that EDS strictly prohibits retaliation against employees for making good faith reports of suspected misconduct.

The Role of EDS as a Global Citizen/Compliance with Laws

EDS acts as a proactive, responsible citizen everywhere it does business. We conduct business in a manner consistent with EDS' guiding set of values, principles and high ethical standards, irrespective of local culture and customs. Valuing what is ethical and doing what is ethical transcend national boundaries and laws. Regardless of the minimums established by local law and custom, EDS will always seek the higher ethical ground when it comes to global issues such as bribery, environmental protection and human rights.

We comply with all laws and regulations that apply in the countries and localities where we do business. Although we may not personally know the details of each of these laws, we should know enough to determine when to seek advice from leaders, local Human Resources or Legal Affairs. Violations of applicable laws and regulations can result in serious civil and criminal penalties for EDS and the individuals involved.

EDS is a global corporation, and we respect the laws in every country where we do business. We also adhere to our own standards everywhere we do business. If you encounter a conflict between the applicable laws of two or more countries, consult with Legal Affairs to determine the best course of action.

Serving Our Clients

At EDS, we strive to treat our clients fairly, honestly, and with respect and dignity. We conduct ourselves professionally and adhere to high standards of integrity everywhere EDS does business.

We are committed to excellence in performance. Our specific commitment to each client is documented in the client agreement. Employees responsible for managing client agreements should be familiar with the terms and conditions of those agreements.

Our clients are the center of our business. Meeting their needs - honestly and ethically - is essential for our success.

Q: ***My client contact asked me for some confidential information about another EDS client. What should I do?***

A: ***While you should always be respectful and courteous, you should absolutely refuse to provide one client with information about another client. Providing information in a situation like this could violate the terms of our agreement with the other client, and it would be unprofessional. If you find yourself in a situation like this, consult your leader or Legal Affairs for guidance.***

Preserving Confidentiality

We must maintain the confidentiality of confidential EDS information and the confidential information entrusted to us by our clients, our employees and other parties, except when disclosure is authorized or legally mandated. When using and managing confidential EDS information, refer to the Security Policy. When using and managing confidential client or other party information, follow the specific rules and obligations that are set forth in the written agreement with the client or other party.

We should be particularly careful when discussing or conducting business in public places such as airplanes, restaurants, social gatherings, elevators and taxis. Use good judgment and comply with company security requirements when using mobile phones, the Internet, wireless communication devices, speakerphones and other forms of unsecured communications.

Our obligation to protect confidential EDS, client, employee and other party information does not end when we separate from EDS employment. We have a continuing obligation – even after we leave EDS – to protect confidential EDS, client, employee and other party information obtained while employed.

For more information on this topic, see the Security Policy, the Information Handling Security Policy, the Use of Corporate Assets Policy, the Financial Integrity Policy and the section titled "Obligations Relating to Prior Employment" contained in this Code.

Do not discuss confidential information with family members or social acquaintances or in places where the information may be overheard. Do not disclose confidential information to another EDS employee unless the employee needs the information to carry out business responsibilities.

Q: ***What is confidential information?***

A: ***Confidential information is information about things such as business plans, operations or "secrets of success" that is not known to the general public or to competitors. It includes all non-public information that might be of use to competitors or harmful to the owner of the information, if disclosed.***

Communicating Openly (Open Door)

Occasionally, each of us will have suggestions for improvements at work or the need to discuss an issue affecting our work lives. You are encouraged to use the Open Door to make suggestions, share insights, or obtain advice and guidance in challenging work-related situations.

For more information on this topic, see the Open Door Policy.

It is only through the invaluable input of our thousands of employees that EDS has grown to what it is today. Every time you make a suggestion, seek guidance or report misconduct, you help EDS become a better place to work.

Q: ***What is the Open Door?***

A: ***The Open Door Policy allows you to talk to any leader in the company about any work-related issue or idea without fear of retaliation. You can also use the Open Door to discuss questions about EDS policy and practices.***

Personal Privacy/Data Protection

As a world leader in the provision of information technology services, and with employees and clients spanning the globe, EDS recognizes the importance of protecting personal data.

EDS respects the privacy and dignity of all individuals and complies with applicable privacy and data protection laws. As an employer and data user and as a provider of information technology services, EDS takes the responsibility associated with data protection seriously.

Personal information of EDS employees, suppliers and directors necessary for effective business operation is collected, shared as appropriate for legitimate business needs and retained in compliance with applicable law. EDS limits its sharing of personal information (excluding employee business contact information) to other employees and to third parties who have written agreements with EDS to protect personal information or who are legally required to protect personal information. Employees who are provided access to personal information must not disclose or use personal information in violation of applicable law or EDS policy.

With regard to employment verifications, as may be required in many countries, certain employee information may be disclosed without the written consent of the current or former employee. Such information includes verification and dates of employment, job titles and work locations. In addition, EDS will disclose any information required by law or court order.

Employee privacy can become an issue when personal use is made of EDS resources. We should have no expectation of privacy when using EDS resources such as company equipment and computer or telephone systems, whether for business or personal use. EDS reserves all rights, to the fullest extent permitted by law, to inspect the company's facilities, property, records and systems, including electronic systems, and the information contained in them, with or without advance notice to employees.

While EDS may from time to time take or use photographs, videos or audio recordings of its employees for business purposes in compliance with applicable law, you may not take or distribute photographs, videos or audio recordings of EDS employees, unless it is clear they consent. Photographing, videotaping or audio recording employees without their awareness or consent may jeopardize their privacy and may violate applicable laws.

For more information on this topic, see the Use of Corporate Assets Policy, the Global Privacy and Data Protection Policy, the Financial Integrity Policy, the Security Policy, the Information Handling Security Policy, Enterprise Security Policies & Standards (ESPS), the Employment Verification site for U.S., and the section of the Code titled "Computers and Equipment, Network Security, Photographic and Audio Devices."

Q: ***Will personal information that I put on EDS' computer systems remain private if I password-protect it?***

A: ***No. To the extent permitted by applicable law, EDS reserves the right to review all information stored on its computer and other systems, even if it is stored under a personal identification code or password.***

Obligations Relating to Prior Employment

In your previous employment, you may have learned, or been given access to, confidential information belonging to your prior employer and its clients or suppliers, and you may have entered into certain enforceable agreements. You are required to honor any such agreements and abide by any applicable laws, including those regarding: (1) disclosure or use of confidential information; (2) hiring/soliciting from the prior employer, and; (3) soliciting the prior employer's clients.

If you have confidential information from a previous job, do not use it for your job at EDS and do not disclose it to your EDS colleagues.

Q: ***Someone from a competitor just joined our organization. I would love to get some information about a proprietary business process that I know her former employer uses. Is it okay if I ask?***

A: ***No, it is not okay for you to ask, and it would not be okay for her to tell you. It is inappropriate to try to obtain our competitors' proprietary information from their former employees.***

Treatment of Employees

EDS is an equal opportunity employer and strives to treat its employees with respect and dignity. Our diverse workforce provides many benefits including creativity, variety in approaches to problem solving and the ability to work effectively as a global company. EDS selects and places employees, without discrimination, on the basis of their qualifications for the work to be performed. This policy applies to all personnel actions, including recruitment, hiring, placement, promotion, separation, compensation, benefits administration, training, education, social and recreational programs, and the use of EDS facilities. The laws of different countries vary regarding employment requirements and practice; therefore, please check with the local Human Resources organization for details specific to your geographic region.

For more information on this topic, see the Diversity and Equal Employment Policy.

EDS is a global and extremely diverse company. We respect and value our differences, both because it is the ethical thing to do and because these differences add value to the company.

Q: ***I've been passed over for several promotions, which I thought I should get. I'm starting to feel as if I'm being discriminated against. What should I do?***

A: ***First, try speaking with your leader about the qualifications and performance necessary for the promotion and what you need to do to be considered. If you do not get the information you need or you still feel as if you are being discriminated against, you are encouraged to utilize the Open Door or contact Human Resources or the Ethics Helpline right away.***

Sexual Harassment and Other Unlawful Behavior

EDS does not tolerate sexual harassment or other unlawful behavior in the workplace, whether committed by a co-worker, leader, client, contract laborer, supplier or anyone else. Actions, words, jokes or comments that are derogatory and based on any person's gender, race, ethnicity, sexual orientation, gender identity, age, religion or disability will not be tolerated at EDS. Although sexual harassment appears in various forms and degrees, it generally consists of unwelcome sexual advances, unwelcome requests for sexual favors or other unwelcome verbal or physical conduct of a sexual nature. Sexual harassment occurs when submission to or rejection of sexual advances adversely affects your employment (for example, promotion or termination) or when unwelcome sexual conduct unreasonably interferes with your job performance or creates an intimidating or hostile work environment.

Regardless of legal definitions or requirements, EDS expects every member of its global family to treat every other member with dignity and respect. If you think you or a colleague is being subjected to workplace harassment, it is extremely important that you notify the appropriate people.

If you think you have been subjected to harassment at EDS, you must report the conduct to any EDS leader with whom you are comfortable speaking about the matter, Employee Relations, the Office of Ethics and Compliance, Human Resources, Legal Affairs, or the Ethics Helpline. No matter which method you use to report your concerns, EDS prohibits retaliation against you in any way for making a good faith complaint.

Complaints of sexual harassment or other unlawful behavior are serious matters. EDS expects employees to report such behavior and leaders to promptly act upon such allegations. If an investigation confirms improper conduct occurred, EDS will take appropriate action.

Contact Employee Relations or the Office of Ethics and Compliance for training and materials on sexual harassment.

For more information on this topic, see the Sexual Harassment Policy and the Violence in the Workplace Policy.

Q: ***A colleague often tells sexually explicit and other questionable jokes. I'm not comfortable saying anything to my colleague. What should I do?***

A: ***If you don't feel comfortable talking to your colleague about the need for this inappropriate behavior to stop, contact your colleague's leader or any EDS leader, Employee Relations, the Office of Ethics and Compliance, Human Resources, Legal Affairs, or the Ethics Helpline.***

Maintaining a Healthy Work Environment

EDS wants its employees to have a healthy, safe and secure work environment as free as possible from known health and safety hazards. Every employee is responsible for using EDS equipment and materials (including cell phones and other portable devices) in a safe manner, exercising good and practical judgment. You are also responsible for immediately reporting accidents, unsafe practices or conditions, and potentially volatile workplace situations to your leader. Other avenues for reporting include the Chief Security & Privacy Office, Human Resources, the Office of Ethics and Compliance, and the Ethics Helpline.

To help maintain an environmentally safe and healthy workplace, EDS complies with all applicable environmental laws and regulations. You are encouraged to contact your leader for assistance if you are concerned about environmental issues or conditions at work.

If you become aware of any potential safety hazard, immediately notify your leader.

Violence in the Workplace

EDS does not tolerate violent acts or threats of violence made by an employee against another person or that person's family or property.

Possession of weapons or other dangerous devices by any person, excluding authorized security personnel, at any time on EDS or client premises is strictly prohibited (unless such prohibition is contrary to local law).

For more information on this topic, see the Security Policy and the Violence in the Workplace Policy.

You may not bring weapons or firearms, including but not limited to rifles, onto EDS' or our clients' property (including all grounds and parking areas).

Q: ***If I'm concerned about a violent situation in the workplace, what should I do?***

A: ***If it is an emergency situation, you should first contact local law enforcement. If your concern does not relate to an emergency, you should contact your leader, the Chief Security & Privacy Office, Human Resources, the Office of Ethics and Compliance, or the Ethics Helpline.***

Drugs and Alcohol

EDS is committed to maintaining a drug-free workplace and prohibits the possession, sale, distribution, manufacture, use, transportation or purchase of any illegal drug or unauthorized controlled substances. You also may not use, obtain or be under the influence of any prescription drug while working other than as medically prescribed. Mood-altering chemicals may impair our abilities and may contribute to a variety of work-related problems.

If you have information regarding the possession, sale or use of illegal drugs or unauthorized controlled substances on EDS or a client's premises, you are obligated to contact your leader, the Chief Security & Privacy Office, the Office of Ethics and Compliance, or the Ethics Helpline.

EDS prohibits working while under the influence of alcohol. Consuming alcohol during work time or on EDS property is prohibited unless the senior leader of your business or support organization, as designated in the EDS Organization Chart published on infoCentre, has given prior approval and proper business decorum is maintained. If alcohol is served at an EDS-sponsored or work-related event, regardless of location, it is permissible to consume alcohol, provided proper business decorum is maintained. Prior approval from the senior leader of your business or support organization is required before EDS pays for or reimburses the cost of serving alcohol at an EDS-sponsored event. Contact Human Resources for local or regional details regarding the possession or consumption of alcohol on client premises.

For more information on this topic, see the Substance Abuse Policy.

Q: ***Can we serve alcohol at an EDS party or special event?***

A: ***With appropriate authorization from the senior leader of your business or support organization, as designated in the EDS Organization Chart published on infoCentre, you can serve alcohol. It is important when alcohol is served at company functions that you not drink excessively and that you behave appropriately.***

Employees must be free from the effects of alcohol or illegal drugs while working. If you are having a drink at a company function or business dinner, use good judgment. Do not drive while under the influence of alcohol – if you have any doubt about your ability to drive, ask a colleague for a ride or take a taxi. Similarly, if you have doubt about someone else's ability to drive, provide the person a ride home or call a taxi.

Conflicts of Interest

As an EDS employee, you make business decisions on behalf of EDS every day. Every decision should be based on the needs and best interests of EDS, and not on any personal interest or relationship.

EDS considers its reputation for integrity a priceless asset. To protect EDS' reputation and our own personal integrity, we must ethically handle conflicts of interest and even the appearance of a conflict. A conflict of interest is just what the name implies – it occurs when you have an outside (non-EDS) interest that conflicts with the best interests of EDS. A conflict of interest can arise from any type of relationship, arrangement or situation that impairs our ability to make decisions on behalf of EDS. The responsibility to ethically handle conflicts requires that you always fully disclose any conflicts to your leader and abide by any conditions placed on you to control or eliminate the conflict. Appropriate conditions may include, for example, removing you from decision-making on behalf of EDS when the decision will or appears to affect your outside interest or having you dispose of the outside interest that creates the conflict or another action.

While most EDS employees must notify their leaders regarding any actual or apparent conflict of interest, special rules apply to certain officers and directors of EDS. Before engaging in any conduct or transaction that creates a conflict of interest, such executive officers and directors must make full disclosure of all facts and circumstances to the General Counsel. If it is not possible to disclose the conduct or transaction before it arises (e.g., in the event that a conflicting interest is unexpectedly inherited), then the officer or director must make full disclosure as soon as possible under the circumstances.

What follows are some common examples of conflicts. It is impossible to specify every situation where a conflict could arise or when it might appear to others that a conflict exists. It is also impossible to specifically address all the potential responses to any given situation. As such, the following represent only examples of appropriate company responses. If you have a question, you should consult your leader, the Office of Ethics and Compliance, or Legal Affairs.

For more information on this topic, refer to the Conflicts of Interest Policy.

Q: ***We are looking for a company to supply our building with coffee, tea and other beverages. We've already spent a lot of time looking. My sister owns a company that provides just this type of service, and I know she would give us a good deal. Can't we just go with her company?***

A: ***No. Hiring a company because your sister owns it or because you trust your sister violates EDS policy. The situation poses a conflict between your desire to get the best deal for EDS and your desire to help your sister. If, however, you disclose your relationship with your sister's company and remove yourself from the selection process, it may be possible for your sister's company to compete for the business along with other suppliers, so long as no one who reports to you is involved in the selection process and you have approval from your leader to submit your sister's company to the appropriate parties for consideration.***

Outside Employment

Because EDS has clients, suppliers and other business relationships in different industries and settings, outside employment may create or appear to create a conflict of interest. As a result, while working for EDS, you must obtain approval from your leader before performing an additional job outside of EDS.

You may not serve as a director, officer, employee or consultant to a competitor of EDS.

Q: ***My dad has a small business that I occasionally do work for. Can I use EDS computers to do work for my dad's business?***

A: ***No. You cannot use EDS resources – including e-mail and telephones – to do work for outside business interests, even if the business interests belong to you or members of your family. Limited and reasonable use of EDS resources for the purpose of performing duties associated with approved service on professional and trade associations, charities and community service organizations, and outside directorships is permitted.***

If your leader approves outside employment, remember that your primary commitment is to EDS. You should not use EDS time or resources in any outside employment, and the employment should not adversely affect your judgment, decisions or ability to meet EDS responsibilities.

Professional and Trade Associations

EDS encourages participation in professional and trade associations in accordance with personal and company interests. If you participate in an outside organization, be sure you understand whether you are representing the company or acting in your personal capacity and make sure the organization understands your role. Only the senior leader of your business or support organization, as designated in the EDS Organization Chart published on infoCentre, can authorize you to act as a company representative to an outside organization.

As a member of a trade or professional group, you may come in contact with competitors' employees. Never discuss proprietary or sensitive competitive issues such as prices, costs, terms or conditions of sale or service, product plans or any other competitively sensitive or non-public information in these settings.

Charities and Community Service

You are encouraged to make contributions of personal time or financial resources to charitable, educational and community-service organizations. You must, however, be alert to possible conflicts of interest between EDS and the organization. If an organization you are involved with seeks to do business with EDS – for example, a charity that is contemplating retaining EDS' services – you must make full disclosure to your leader. You will likely be required to disqualify yourself from making or participating in any decision on behalf of EDS that concerns or impacts the charity. For more information on contributions to charities and community-service organizations, contact EDS Global Community Affairs.

Even contributions to charities and community organizations can create conflicts of interest and require compliance with applicable laws.

Q: ***I would like to donate some of EDS' outdated computers to a charity that is supported by one of our clients. Can I do that?***

A: ***Possibly, but you must obtain approval from EDS' Global Community Affairs before making any contribution of corporate resources for charitable or community purposes in any location. Contributions of EDS' time and financial resources to non-profit organizations can create conflicts of interest as well as present legal and regulatory concerns.***

Outside Directorships

EDS considers your time, talent and energy essential to our success. Generally, EDS does not encourage its employees to serve on boards of directors of outside, for-profit organizations. Such service, however, may be approved in selected cases. Prior to joining the board of any external for-profit organization, you must obtain approval in accordance with our policy for approving board seat service by employees. As a condition to approval, terms may be imposed on your outside board service, including remuneration, indemnification and insurance coverage.

For more information on this topic, see EDS' Conflicts of Interest Policy.

When serving as a director or officer of any non-EDS entity, you must avoid any conflicts of interest between your roles at EDS and the other organization.

Service as a director of a for-profit organization requires prior approval. Service as a director of a competitor is prohibited. Service as a director of a civic, charitable or other not-for-profit organization does not require leadership approval but does require that you notify your immediate leader prior to accepting the position.

Q: ***One of my fraternity brothers from college owns his own business, and he has asked me to serve on its board of directors. They do not do business with or have any connection with EDS. Can I help him out?***

A: ***Possibly, but you must first obtain approval in accordance with the policy for approving board seat service by employees.***

Personal Investments

Personal investments can create conflicts of interests if you need to make a decision for EDS concerning companies in which you or an immediate family member has a personal economic interest. Such conflicts could arise if you own stock in a company that already is or seeks to become a supplier, client or strategic ally of EDS. A conflict of interest arises if:

- The investment is significant to you and a reasonable person would conclude that your judgment in making decisions for EDS could be affected, or
- The transaction with EDS that you have decision-making authority for is such that it could affect your economic interest in the other company.

If you or an immediate family member has a substantial pre-existing investment in a company and then you become the EDS decision-maker with respect to that company, you should promptly disclose that ownership interest to your leader. Your leader will then determine what measures are necessary to control or eliminate the conflict.

You should not make substantial investments in another company at a time when you are making decisions for EDS concerning the other company.

Q: ***I own shares in a company that has recently become a supplier to EDS. Is that a problem?***

A: ***It may be, if the investment is substantial enough and you make or participate in making decisions for EDS that concern the supplier. Conflicts may arise if you or an immediate family member has a substantial interest in or relationship with a company involved in a transaction with EDS and you are a decision-maker with respect to the transaction.***

Business Opportunities

You must not take for yourself opportunities that are discovered through the use of EDS' property or information or through your position at EDS (such as from an EDS client) without first offering the opportunity to EDS. Such opportunities could include options to purchase stock in other companies, the opportunity to purchase stock in other companies at below-market prices, and other investment opportunities. Business opportunities are corporate assets, and they should not be taken personally without disclosure and approval of your immediate leader and the Office of Ethics and Compliance. You also must not use EDS' property or information or your position at EDS for improper personal gain.

You must not engage in any activity, directly or indirectly, that competes with EDS' interest. If you become aware of any such activity, you should bring it to the attention of your leader or the Office of Ethics and Compliance.

If you learn of a business opportunity through your work at EDS, before you or an immediate family member acts on the opportunity for personal benefit, you must first disclose the opportunity to your leader and offer the opportunity to EDS.

Q: ***I've been working on-site at a client's offices for the last six months, and I've become friends with its head of business development. When I was at the client's offices yesterday, my friend told me about a great opportunity to invest in a small, privately held company that the client often uses. The client is also planning to invest. Can I make the investment?***

A: ***Not without first presenting the opportunity to your leader and obtaining the approval of the Office of Ethics and Compliance. Because you learned of this investment opportunity through your work for EDS, the opportunity belongs to EDS and should first be offered to EDS.***

Family and Personal Relationships at EDS

The employment of relatives may raise questions regarding confidentiality, objectivity and integrity in work relationships. In order to promote integrity in our employment relationships, and unless contrary to applicable law, you must immediately disclose to your leader any relative or personal relationships with others who work at EDS or who are being considered for employment by EDS. EDS may permit relatives or those in a personal relationship to work in the same unit provided that neither of these individuals is the immediate manager of the other or directly involved in employment-related decisions, such as assignments, compensation, performance reviews, disciplinary actions or promotions, of the other person. Where one of the employees is an EDS leader in the same reporting line, the potential for the appearance of improper influence is high and therefore at least three levels of supervisory authority should exist between the leader and the relevant employee, if possible.

For more information, see the Conflicts of Interest Policy.

You may not make or participate in a hiring or placement decision if the applicant or employee is a member of your immediate family or in a personal relationship with you. If you find yourself in such a situation, disclose the situation to your leader and refrain from participating in the decision.

All employment-related decisions – including hiring, promotion, compensation, employment reviews, disciplinary action and termination – must be made objectively and without regard to personal interests, including the interests of family members. Even if you believe a decision involving a relative or other personal relationship is based on EDS' best interests, you must avoid the appearance of impropriety.

Q: ***Does EDS' Conflicts of Interest Policy apply to distant relatives, such as cousins, or to friends?***

A: ***The policy typically applies only to members of your immediate family, which includes any child, stepchild, parent, stepparent, spouse, sibling, mother-in-law, father-in-law, son-in-law, daughter-in-law, brother-in-law or sister-in-law, and any person sharing your household or dependent on you or your spouse for financial support. For purposes of conflicts of interest, people with whom you are in a personal relationship are also considered immediate family. The general rule, however, is that you should avoid the appearance of impropriety. If conduct or decisions on behalf of EDS that involve a distant relative or friend look inappropriate, you should abstain from the conduct or from making the decision without first disclosing it to your leadership and getting appropriate approval.***

Family and Personal Relationships Involving Other Companies

You may have an immediate family member who works for a competitor, supplier or client of EDS. Such situations are not prohibited, but they call for extra sensitivity to confidentiality and conflicts of interest.

Unless prohibited by law, if you have an immediate family member who works for a competitor, supplier or client, you must disclose your specific situation to your leader to assess the nature and extent of any concern and how it can be resolved.

If a member of your immediate family is employed with any business selling to, buying from or competing with EDS, you must be especially careful not to disclose EDS confidential information. Your leader may also impose other controls, including requiring that you not be involved in decisions on behalf of EDS that involve the other company. EDS will work with you to ensure everyone's interests are protected.

Exchanging Gifts and Other Business Courtesies

While the exchange of business courtesies can help build business relationships, accepting or providing business courtesies that are excessive or inappropriate can harm your reputation and the reputation of EDS. You must use your judgment to distinguish between appropriate situations that build relationships and inappropriate situations that create or appear to create conflicts of interest or violate applicable law.

The following rules, together with those set forth in the Conflicts of Interest Policy, should guide you in accepting and giving gifts or other business courtesies.

With respect to non-government business, you may accept or offer gifts and business courtesies, including meals and entertainment, so long as they are customary and commonly accepted business courtesies, not excessive in value, and given and accepted without an express or implied understanding that the recipient is in any way obligated by acceptance of the gift. Gifts that are excessive in value should not be accepted or given without the approval of your leader or the Office of Ethics and Compliance. If you have a question about the value of a gift, consult with the Office of Ethics and Compliance. You must never ask for gifts, entertainment or any other business courtesies from people doing business with EDS.

See the "Bribery and Improper Payments" section of this Code for more restrictive rules that apply to EDS individuals doing business with political parties, governments and government-owned entities (including gifts and business courtesies exchanged between private companies that are working on a government contract as a prime contractor and subcontractor).

For more information on this topic, see the Conducting Business with Government Entities Policy, the Financial Integrity Policy, the Conflicts of Interest Policy and the EDS Policy for the Prohibition of Corrupt Payments.

Q: ***In my country, refusing a gift from a business associate can be considered an insult. What should I do if I am offered an expensive gift and know that I will cause offense if I don't accept it?***

A: ***If it is customary to exchange gifts in the local culture and you believe that you will harm EDS' business relationships if you do not accept a gift, you may accept the gift on behalf of the company. You must then disclose the gift to your leader to determine appropriate disposition.***

Q: ***Do all government agencies have the same rules regarding accepting meals and entertainment?***

A: ***No. The rules differ among different governments and government agencies. This area can be extremely complicated. Before providing any meals, entertainment or other business courtesies to a government official, you must check with Legal Affairs.***

Gifts and entertainment that are typically okay:

- Pens
- Calendars
- Memo pads
- T-shirts
- Coffee mugs
- Occasional lunch or dinner at a restaurant
- A local sporting event or entertainment

Gifts and entertainment that require pre-approval:

- Travel expenses (such as airfare and lodging) paid by a third party
- Trips or tickets to extravagant sporting events, such as the Super Bowl, the World Cup, the Masters, the Olympics, etc.
- Frequent gifts from the same source, even if each individual gift is moderate
- Gifts exchanged with government officials
- Gifts exchanged between prime contractors and subcontractors on a government contract

Cash is never okay.

Solicitation/Distribution

In the interest of a professional work environment and to protect EDS' employees and directors from unwanted solicitations, you may not solicit or distribute any non-work-related literature for any purpose during your working time or the working time of the person(s) you are soliciting. You may not distribute literature at any time in any work area. In addition, selling, trading, or bartering of services or merchandise to others is prohibited on EDS premises during work time. Consistent with federal law, the company may permit a small number of solicitations for charitable causes, as determined by the senior leader of your business or support organization, as designated in the EDS Organization Chart published on infoCentre. Participating in or soliciting for organized or commercial lotteries or other gaming or gambling activities is prohibited.

Persons who are not employees may not solicit or distribute literature for any purpose on EDS premises at any time, unless they have the approval of the senior leader of the business or support organization, as designated in the EDS Organization Chart published on infoCentre.

This policy should not be construed as prohibiting or restricting solicitation/distribution that is otherwise permissible under federal labor law.

EDS maintains a professional work environment. Do not solicit your colleagues or EDS clients for non-EDS products or services or for religious, political or charitable causes during work time.

Q: ***I sell cosmetics on the weekends and in the evenings. Can I sell to other EDS employees or clients?***

A: ***You cannot sell to other EDS employees in the workplace or on work time, and you should never solicit EDS clients for personal business interests during work time.***

Media Inquiries/Public Speaking/Published Works

Before answering any questions or speaking with the media, you must contact EDS Corporate Public Relations. They will advise you on the proper action and may handle the contact directly and/or be present during any conversation. In matters of litigation or potential litigation, only the Office of the Chairman, Legal Affairs and EDS Corporate Public Relations are authorized to speak with the media. In these cases, you must refer media directly to EDS Corporate Public Relations.

Speeches and published works, such as books and magazine articles, offer excellent opportunities for EDS to present topics and ideas of interest to business and professional audiences. Any speech or published work on a professional topic by an EDS employee could be perceived to represent EDS' position. Therefore, such speeches and published works must be pre-approved before any company time or resources are committed to them and before they are released. Pre-approval must be obtained from the Office of the Chairman if there is the possibility of a national audience. Pre-approval must be obtained from the senior leader of your business or support organization, as designated in the EDS Organization Chart published on infoCentre, if there will only be a local audience.

Because EDS is a publicly traded company, we are governed by laws and regulations regarding how we disclose significant events to the public. That is one reason why it is important that we confer with authorized personnel before answering the media's questions.

Q: ***A local reporter called asking for information about EDS. Can I talk to the reporter?***

A: ***Not without first consulting EDS Corporate Public Relations. Talking to reporters can be harmful to the company if you don't have all the facts, and it can also implicate securities laws.***

Contracting and Signing on Behalf of EDS

When we enter into agreements or sign documents on behalf of EDS, we can create legal obligations and legal and financial risks for the company. Correspondence, reports and other documents that contain substantive opinions, conclusions or determinations or that legally bind EDS must be signed by or under the control of EDS leadership. Before you sign an agreement for EDS, be certain that you have the legal authority to obligate the company and that you have all required corporate authorizations, including any required authorizations under the Signatory Authorization Process.

Special issues arise when we contract with the U.S. government. For more information on this topic, see the Financial Integrity Policy and the section titled "Contracting with Government Entities" contained in this Code.

Never sign on behalf of EDS unless you have the appropriate signatory authority and approvals.

Assisting Others in Misconduct

EDS is committed to acting with the utmost integrity in all of our business dealings. We will not knowingly assist a client, supplier or any other person or entity in violating or avoiding legal or regulatory obligations, including disclosure and financial obligations under the securities laws. Our business dealings should be transparent, and the documents we use to record a transaction should accurately reflect the deal that was negotiated. This means, for example, that we will not provide false or misleading statements about our business dealings with a client to its auditors, nor will we put portions of our business arrangements into separate "side letters" if we believe a client's purpose is to hide the letter from its auditors or otherwise keep it from receiving appropriate visibility within the client's organization. If you are asked to participate in or become aware of any such arrangements, or if you are not sure whether a particular arrangement may be improper, discuss it with your leader, Legal Affairs, the Office of Ethics and Compliance, or contact the Ethics Helpline right away.

Ask questions to ensure that you are not assisting others in conduct that will violate or avoid legal or regulatory obligations.

Q: ***I've been negotiating a two-year contract with a potential client for the last five weeks. Recently, the client requested that we agree to a contract provision that states EDS will provide certain services to the client only in year two of the contract – yet it is well understood that EDS will provide services in both years of the contract. Can EDS agree to this term and nevertheless provide services in both contract years?***

A: ***No, to agree to this term would be inconsistent with the underlying business arrangement and may allow the client to inappropriately account for the transaction. You should question contract terms, including statements of work and payment arrangements, which seem to distort or conceal the underlying business arrangement.***

Protecting EDS Assets

You must safeguard EDS assets from loss, misuse, waste, damage and theft and use them efficiently. Failure to do so has a direct impact on EDS' profitability. "Assets" are all the resources owned or controlled by EDS.

Q: ***I am an administrative assistant, and I am filling out my leader's expense report for a recent business trip. I know my leader's spouse, who is not an EDS employee, went on the trip and that the spouse's expenses are included in the report. What should I do?***

A: ***If you're comfortable doing so, you can ask your leader if the spouse's expenses were included by mistake. If you're not comfortable asking, you must report the matter to your leader's leader, Legal Affairs, the Office of Ethics and Compliance, or the Ethics Helpline. Remember that part of your job is to help EDS protect its assets and resources; reporting this matter is one of your responsibilities as an EDS employee.***

Q: ***After work, I sometimes go directly to the gym. I always take my laptop home, so while I'm in the gym, my laptop is on the front seat of my locked car in the parking lot. Is this okay?***

A: ***No, it is not. You should only take your laptop home if it's necessary for your EDS work or if there is no way for it to be safely left at work. You must safeguard your laptop and the data it contains; leaving your laptop on the front seat of your car in this situation is not safe. If you need your laptop at home, take it there first or go back to your office and get it after you're finished at the gym. If these options won't work, and you think it's safe, lock the laptop in the trunk of your car when you leave work rather than when you get to the gym, park in a highly visible section of the parking lot and keep an eye on your car.***

Examples of EDS assets, which we all have a responsibility to protect, include:

- Offices
- Buildings
- Equipment
- Computer systems
- Supplies
- Corporate funds
- Financial data
- Corporate records
- Intellectual or intangible property, such as technologies, ideas, information, inventions, concepts, business practices and methods, strategies and plans, client and employee lists, and business opportunities
- The time and talent of EDS employees

Proper Use of Corporate Assets and Resources

EDS assets are intended to help us achieve business goals. Careless or inefficient use of company assets hurts all of us.

EDS permits limited and reasonable personal use of basic office services and systems such as telephones, photocopiers, facsimile machines, personal computers, and access to the Internet and other public networks. Personal use of corporate resources is a limited privilege, not an entitlement. When using EDS assets or resources for personal use, you should exercise good judgment and keep personal use to a minimum. Where not prohibited by law or regulation, EDS reserves the right to monitor the use and content of its assets and resources.

Personal use of EDS assets or resources must:

- Comply with laws and regulations and EDS corporate policies
- Not interfere with work responsibilities or service to clients
- Not interfere with required business communications
- Not be used in the support or operation of a business other than that of EDS
- Never be used in a manner or for a purpose that would reflect unfavorably upon EDS' reputation, such as use in pursuit of illegal, unethical or otherwise questionable goals, or to access or communicate offensive, vulgar or pornographic material

You must also abide by all security procedures and controls to protect the integrity and security of EDS data and networks.

Limited and reasonable use of EDS resources for the purpose of performing duties associated with approved service on professional and trade associations, charities and community service organizations, and outside directorships is permitted.

For more information on this topic, see the Use of Corporate Assets Policy, the Financial Integrity Policy and the Security Policy.

Q: ***I use my Internet connection at work to check my stock portfolio. Is there any problem with that?***

A: ***Limited personal use of the Internet – such as checking your stock portfolio on occasion – is acceptable. You should not, however, spend more than a very limited amount of time doing personal tasks at work. Your use of the company's time and resources in this manner takes away from the time that you would otherwise be devoting to EDS.***

Software and Other Protected Intellectual Property

As a provider of information technology services, it is important for EDS to comply with copyright and intellectual property laws. Do not violate license agreements and do not use unlicensed software on EDS' systems.

You should not use unlicensed or illegal copies of software. In addition, EDS licenses many computer programs owned by third parties. Our policies require you to respect the copyrights of others and use software licensed to EDS in conformance with applicable license agreements. Violation of a software license agreement could result in legal liability against both EDS and the responsible individual.

Other types of intellectual property, such as music, literary works, photographs, film, video and other published material, also have legal protection under most countries' laws. Before you download, use, distribute or copy such property, check with Legal Affairs to be sure that EDS has the legal right to do what you propose.

For more information on this topic, see the Use of Non-EDS Software Policy, the Financial Integrity Policy and the Security Policy.

Q: ***Our organization purchased a site license from a software company for a new computer program. A friend in another organization wants to use it and asked if I would make a copy. It would be for business use. Can I make the copy?***

A: ***No. When a license agreement with a software supplier restricts the use of a program to a particular organization or site, we cannot make copies that violate the license agreement. Even copies for other EDS organizations may violate a license agreement.***

Computers and Equipment, Network Security, Photographic and Audio Devices

Public electronic networks such as the Internet raise the potential for unauthorized access to e-mail and other files transmitted over such networks. Data security over public networks simply cannot be guaranteed. Therefore, take care to ensure sensitive information is sufficiently protected before it is routed through the Internet or other public networks.

The physical security of our network and equipment is everyone's responsibility. You must protect and secure this equipment at all times. You must protect the confidentiality and integrity of information used to access our networks, including IDs and passwords, hand-held authentication devices, pass codes, and building-access key cards. The same precautions should be taken to protect computer systems, including client, supplier and EDS data, application software and audit logs, and files for audit and recovery. You should log off the network or activate a password-protected screensaver whenever you leave your computer terminal or data device unattended or unsecured.

You may not use any type of photographic, video or audio recording device at an EDS or client facility to capture proprietary information about security equipment or procedures unless specifically authorized by the Chief Security & Privacy Office. The unauthorized use of these devices in the workplace poses a serious risk to both information security, and employee and facility security. Photographic images and audio recordings of EDS proprietary information regarding business processes, software designs and so forth could allow third parties to access and misappropriate our intellectual property or compromise the integrity and availability of our resources.

For more information on this topic, see the Use of Corporate Assets Policy, the Global Privacy and Data Protection Policy, the Security Policy, the Information Handling Security Policy, and the section of the Code titled "Personal Privacy/Data Protection."

Q: ***I found some free software on the Internet that I would like to use on a project. Can I install it on my company laptop?***

A: ***You may only use public domain or freeware software if you first obtain your leader's approval. Note that "shareware" software is not in the public domain and is not necessarily free; it generally is subject to license terms. Do not use shareware without first obtaining your leader's approval and advice from Legal Affairs.***

- Our network security is the responsibility of every employee who uses the network. Safeguard your passwords and IDs and all hand-held devices, and take your responsibility seriously.
- Do not install or use unauthorized software on any EDS computer.
- Never provide your password to anyone – inside or outside the company – nor record it somewhere that it might be accessible by others.
- Do not use photographic, video or audio recording devices without proper authorization.

Electronic Communications

Whether communicating face-to-face or by means of electronic communication tools such as the computer, telephone, fax, voice mail, mobile messaging or other wireless communication devices, each of us must communicate professionally. EDS will not tolerate the use of its communications and messaging tools (including the Internet and intranet) to send, retrieve or store harassing, threatening, derogatory, defamatory or obscene messages or other such communications to anyone. Use of communication tools to send "chain letters," hoax notices or other such communications is not professional business behavior and is prohibited.

Sending technical data via the Internet or intranet to another country or, in some instances, to a national or citizen of another country, involves the export/import laws of both the transmitting and receiving countries. Similarly, many jurisdictions restrict certain commercial uses of electronic communications (like spam or telephone solicitations), and privacy laws may be impacted if any personal information is communicated. Never use electronic communication tools for commercial uses, such as mass faxing, mailings or telephone solicitations without first checking with Legal Affairs.

For more information on this topic, see the Export/Import Laws Policy, Use of Corporate Assets Policy, the Financial Integrity Policy, the Global Privacy and Data Protection Policy, the Security Policy, and the Information Handling Security Policy.

Q: ***I sometimes use e-mail to send personal messages when I'm at work. Is that okay?***

A: ***Occasional personal use of e-mail is acceptable. You should, however, have no expectation of privacy if you send e-mail using company computers. You also must abide by all company policies when using company computers. You must never send harassing or inappropriate e-mails, chain letters, personal advertisements or solicitations.***

Remember that when you are using company resources to send e-mail or to access Internet services, you are acting as a representative of EDS. Any improper use of these resources may reflect poorly on EDS, damage its reputation, and expose you and the company to legal liability.

Accurate Books and Records and Disclosure

We must each ensure that financial information within our control is recorded accurately and in a timely manner in the company's financial accounts. No false, artificial or misleading statements or entries will be made in reports, business plans, books, records, accounts, documents or financial statements, including the omission of entries if such omissions could be misleading. You must accurately separate and report business and personal expenses. You must record all transactions in a manner that maintains accountability for all EDS assets and permits preparation of accurate financial statements.

EDS' chief executive officer and its senior financial professionals (including its chief financial officer, controller and principal accounting officer) have a special role to play in ensuring appropriate public disclosure of EDS financial information. These executives must adhere to policies and practices that promote full, fair, accurate, timely and understandable disclosures in reports and documents that are filed with or submitted to the United States Securities and Exchange Commission and in other public communications. At the same time, each of us must support such disclosures by ensuring information within our control is not only properly recorded, but fully, fairly and accurately communicated in a timely fashion to appropriate company personnel.

We all have a role in helping to ensure the books and records of the company and its subsidiaries comply with EDS accounting practices and generally accepted accounting principles. No lesser standard is acceptable. Detailed guidelines regarding accounting controls and financial reporting are available to EDS employees on the Finance Web site.

Q: ***The quarterly reporting period ends in two weeks. Our numbers are slightly off-target, and my leader has asked that I record a few sales now that won't be finalized until next month. The sales are pretty much certain to happen. Is there any problem with this?***

A: ***Yes, there is. Revenues must be reported during the appropriate reporting period, and the company's compliance with generally accepted accounting principles may not be compromised. You must report the request to your leader's leader, Legal Affairs, the Office of Ethics and Compliance, or the Ethics Helpline.***

Document Retention

Various laws and regulations and the EDS Records Retention Policy require retention of certain EDS records, including electronic records, for specific periods of time. The subject matter of the record – not its form – determines the appropriate retention period.

You must not destroy records relevant or potentially relevant to pending or expected litigation, tax positions, audits or investigations. If EDS receives a subpoena to produce such records, you must not in any way modify or destroy the records. Unauthorized destruction or falsification of any relevant or potentially relevant records may lead to prosecution for obstruction of justice. If in doubt about the legality or propriety of destroying or changing any document or other record, you should consult with Corporate Records Management and Legal Affairs.

For more information on this topic, see the Records Retention Policy, the Documents and Records Archival site, and the Financial Integrity Policy.

NEVER destroy or alter records that are the subject of litigation or an investigation. It can get you and EDS into serious trouble.

Q: ***Are electronic records, like e-mail, covered by the Records Retention Policy?***

A: ***Yes, all EDS records – including electronic records – are subject to the policy. If you have any questions about specific retention periods, you should consult the EDS Corporate Records Retention Schedules on the Document and Records Archival site or contact Corporate Records Management. In the case of employment records, you should contact Employee Relations or Legal Affairs.***

Insider Trading

"Insider trading" can occur when a person buys or sells securities of a company while aware of material non-public information about that company. Material non-public information is any information that is not yet public and could reasonably be expected to affect the price of a company's securities or be considered important by a reasonable investor.

The law and company policy prohibit insider trading. This prohibition on insider trading applies not only to trading in EDS securities, but also securities of EDS' clients and suppliers or other entities having a business relationship with EDS. These rules also forbid sharing material non-public information regarding EDS or other companies with others who then trade in securities using the information.

The law and company policy may, however, permit you to trade in EDS securities regardless of your awareness of material non-public information if the transaction is made pursuant to a prearranged trading plan complying with applicable law. For additional information on trading plans, contact Legal Affairs.

If you have any doubt as to whether particular conduct may violate the restrictions on insider trading, you should contact the Office of Ethics and Compliance or Legal Affairs.

For more information on this topic, see the Insider Trading Policy and the Financial Integrity Policy.

Q: ***In working with one of our clients, I've learned that the client is on the verge of a big breakthrough that I think will really help the client increase its sales. I want to purchase some of the client's stock. Can I?***

A: ***No. You cannot purchase stock in the client company until the information you have is disclosed to the public.***

Do not disclose material, non-public information about EDS, our clients, suppliers or other entities having a business relationship with EDS to anyone, including co-workers, who do not have a legitimate need to know such information for business purposes. Examples of material information include unannounced financial results and may include information concerning the following situations: sizable new or lost contracts; important personnel changes; major lawsuits; and possible mergers, acquisitions, divestitures or joint ventures.

Communication with Outside Legal Counsel

Legal counsel representing other companies, government agencies or individuals may contact you seeking information about EDS business, our clients, employees or suppliers. To protect employees, directors, clients and EDS in connection with litigation and other legal matters, and ensure any information released is complete and accurate, you must, as a general rule, immediately refer all contacts from legal counsel outside the company to EDS Legal Affairs. Special issues may arise if you are contacted by government investigators. For additional information, see the "Government Investigations" section in this Code.

If in connection with EDS business you receive a subpoena to provide documents or appear as a witness, you must immediately contact Legal Affairs for assistance.

Generally, all contacts from outside legal counsel should be referred to Legal Affairs.

Q: ***I got a call from a lawyer for one of our former clients, asking me questions about my work for this client. The lawyer's questions do not concern EDS; they concern a dispute between the former client and one of the client's former employees. Should I answer the lawyer's questions?***

A: ***No, you should not speak with the lawyer without assistance from Legal Affairs. You should refer the lawyer to Legal Affairs.***

Obtaining Competitor Information

EDS participates in a highly competitive market. We will compete vigorously and fairly and always in an ethical and legal manner. We can gather information about our competitors from sources such as published articles, advertisements, brochures, other non-proprietary materials and surveys by consultants. We will avoid any practice that could result in or be perceived as inappropriately obtaining competitive information, such as theft, spying, bribery or breach of a competitor's nondisclosure agreement.

If there is any indication information you are offered was not lawfully obtained, you should refuse to accept it. If you receive any competitive information anonymously or that is marked confidential, you should not review it and should immediately contact Legal Affairs. Be aware that there are very strict rules that restrict obtaining non-public information from the government.

It is entirely proper for us to gather information about our marketplace, including information about our competitors and their products and services, but we must do so only in legal and appropriate ways.

Q: ***It would be very helpful to me in repricing some of our services to know what our main competitor in this area is charging for the same services. I can't seem to find the information in public documents or on the competitor's Web site. Is it okay if I call the competitor – from home – pretending to be a customer?***

A: ***No. You should never misrepresent yourself in order to obtain competitive information.***

Maintaining the Highest Standards of Integrity in Contracting with Government Entities

Providing services to government organizations is a significant part of EDS' business. The laws, regulations and ethical considerations affecting our interactions with government entities often differ from dealings with non-government clients. We must maintain the highest standards and abide by all pertinent government contracting laws, rules and regulations. Failure to follow applicable rules can result in penalties, contract cancellation, suspension and debarment from future government contracting opportunities.

Anyone involved in selling, implementing or working on government contracts must be familiar with both the general rules of government contracting and the specific requirements applicable to their government contracts. Specific regulations, which may vary with different government entities, will dictate the contracting procedures to be followed. Government contracts do not exempt contractors from complying with the export/import regulations of the countries involved.

For more information on this topic, see the Conducting Business with Government Entities Policy and the Policy for the Prohibition of Corrupt Payments.

Misconduct in government transactions, even when it results from lack of knowledge, can have serious consequences for our business. The rules governing government contracting are complicated. If your organization does not regularly do business with government entities, you should contact Legal Affairs before responding to a request for proposal to provide services to a government entity.

Q: ***The government contract I'm working on requires us to purchase a particular product from a specific supplier. I found a cheaper source of supply. Can I switch?***

A: ***No. You must follow the contract specifications exactly unless you first get the government's written approval to make a change.***

Q: ***I discovered some inaccurate information was mistakenly provided to the government agency client in connection with a contract between EDS and the government agency. What should I do?***

A: ***You should promptly inform your leader, Legal Affairs, or the Office of Ethics and Compliance. They can help you disclose the mistake in the appropriate way.***

Classified and National Security/Official Secrets

Various laws and regulations govern the acceptance, protection, handling, disclosure and control of classified documents and information. You must adhere to all government regulations regarding classified information. You must also respect the strict rules of the government regarding those who may properly have access to and possession of copies of classified or other government data, including classified information entrusted to EDS by governments and their contractors. Each of us who has access to government-classified information must safeguard the security of that information. Report any breach of security immediately to Legal Affairs or the Chief Security & Privacy Office.

Our obligation to safeguard classified information continues until the information is declassified.

Q: ***I know I can only disclose classified information to my colleagues who have the appropriate level of security clearance and a need to know. How do I verify security clearance?***

A: ***Contact the Chief Security & Privacy Office before disclosing the information. They can verify a security clearance level for any EDS employee.***

Government Investigations

As a general rule, investigation and litigation matters are handled exclusively by EDS Legal Affairs, and any documents that relate to an investigation or litigation should be immediately referred to that office. EDS fully cooperates with all government investigations.

While EDS cooperates with government investigations, and in limited instances may provide personal information of employees, it also has important interests to protect. EDS, for example, has confidentiality obligations to its clients, including, in some cases, the obligation to provide notice to the client when requested or ordered to provide information about the client. Accordingly, if a government representative contacts you regarding an investigation, in most instances, you should politely advise the representative that EDS' policy is to fully cooperate in all government investigations and that responses must be coordinated through Legal Affairs. You should then immediately contact Legal Affairs to receive further advice. This process will help ensure the accuracy of the information EDS provides to the government.

There may be instances where contact with government investigators is appropriate. If you have any doubt or concern about the appropriateness of speaking with a government investigator, you may seek guidance anonymously through the Ethics Helpline. Please keep in mind that you are required to report any suspected wrongdoing to the company, and the company strictly prohibits retaliation against employees for making good faith reports of suspected misconduct.

Q: ***I just received a subpoena for certain EDS records from a government agency. What should I do?***

A: ***If you receive a subpoena or other request for EDS, client or supplier documents, you should notify your leader and immediately forward a copy of the subpoena or request to Legal Affairs.***

Never destroy or alter documents in anticipation of a request for them from the government, and always be honest in dealing with government agents and investigators.

Political Contributions and Activities

Laws of certain jurisdictions prohibit the use of company funds, assets, services or facilities on behalf of a political party or candidate. To ensure compliance with applicable laws, each of us must obtain written consent from the Office of Global Government Affairs prior to committing any company time or resources for political activities, including lobbying.

EDS does not restrict your personal participation in political activities or use of personal funds for political purposes. EDS will not reimburse you for any personal political contribution.

For more information on this topic, see the Political Contributions and Activities Policy and the Financial Integrity Policy. Also see the EDS Policy for the Prohibition of Corrupt Payments.

The laws and regulations governing corporate political activities are complex and vary dramatically in different countries and localities. Before engaging in any political activities on behalf of EDS, consult with the EDS Office of Global Government Affairs. This will help ensure the activity or contribution is legal and cannot be misconstrued as having been for any improper purpose.

Q: ***My leader asked me and some others in our group to make a contribution to a friend's campaign for city council. Is that appropriate?***

A: ***No. Even if your leader is not pressuring you, the request is inappropriate. If you are not comfortable speaking to your leader about this, you can speak with your leader's leader, the Office of Ethics and Compliance, or the Ethics Helpline.***

Anti-Money Laundering

Money laundering is the process by which large amounts of illegally obtained money (from drug trafficking, terrorist activity or other crimes) is given the appearance of having originated from a legitimate source. Money laundering is not limited to cash transactions; it also can include, among other things, checks (including traveler's, cashier's or third-party), money orders and all forms of electronic transfers, including transfers of currency and securities. EDS takes seriously its obligation to help close off the channels that money launderers use. If you observe or suspect a money laundering transaction, immediately contact Legal Affairs.

Money laundering is a problem of global proportions with potentially devastating consequences.

Q: ***One of our clients called to say that it is changing banks and needs to pay its most recent bill in cash, because its new account isn't ready. What should I do?***

A: ***Contact Legal Affairs, which will help you assess the situation. Cash payments should typically be considered suspicious and be investigated. Other types of potentially problematic payments include money orders, traveler's checks, cashier's checks, third-party checks or transfers from third-party accounts.***

Bribery and Improper Payments

You must not, directly or indirectly, offer, pay or receive a bribe.

The laws of many countries, including the U.S. Foreign Corrupt Practices Act (FCPA), and EDS policy prohibit us from directly or indirectly giving or offering anything of value to government officials or officials of public international organizations for the purpose of gaining business or favorable government action. Payments need not take the form of cash to be prohibited. They may be anything of value, including gifts or services. Generally speaking, small business courtesies such as reasonable expenses for meals directly related to business promotion or contract performance are not prohibited. Determining what gift or payment may be permitted may involve difficult legal judgments. In addition, in a number of countries there are absolute prohibitions or very tight restrictions on gifts for any purpose to members of the national legislative body, their families and staff. Therefore, do not make any payments or give gifts related to EDS business activities to government officials, officials of public international organizations or members of national legislative bodies, their families or their staff unless the transaction is approved first by Legal Affairs.

In every case, we are required to maintain accurate records and internal controls.

For more information on this topic, see the EDS Policy for the Prohibition of Corrupt Payments, the Conducting Business with Government Entities Policy, the Financial Integrity Policy and the Contractor Compliance Process.

Q: ***While I understand and appreciate EDS' desire to abide by high ethical standards, it is sometimes tough to do that and maintain our competitive standing. I will likely lose a big contract if I don't pay a local official a bribe. Does EDS really want me to lose the business?***

A: ***Yes, EDS would rather lose business if gaining business requires bribery or other improper means. The short-term gain of winning that contract will be more than offset by the long-term loss of reputation and credibility if you get caught, and, more importantly, the contract is just not worth violating the law and our high standards of business ethics. If you are faced with a situation like this, speak to your leader, Legal Affairs, or the Office of Ethics and Compliance. EDS places great value on your decision to act appropriately in difficult circumstances.***

Q: ***I am working with a foreign agent in Asia who is helping me navigate some of the intricacies of contracting with a government there. I am concerned that some of the money EDS is paying the agent may be going toward paying bribes to government officials, but I have no actual knowledge that bribes have been paid. Is this of any concern to EDS?***

A: ***Yes, it is. EDS can be liable for bribes made to foreign government officials, even if they are made by an agent or subcontractor. We cannot avoid liability by "turning a blind eye" when circumstances indicate a potential violation of anti-bribery laws. You should report the matter to Legal Affairs immediately to get assistance in determining if any bribes have been paid. Remember, it is also necessary to perform due diligence on agents or contractors prior to hiring them to help ensure no bribes will be paid.***

Export/Import Control Regulations

EDS conducts its international business in strict compliance with all applicable export/import laws and regulations. Under regulations administered by various export/import control agencies, the export/import of goods, software, services or technology from a country in which EDS conducts business may require a specific export or import authorization. In some cases, the export laws of a country will continue to apply to the movement of items or technology, even after the items or technology have been exported from that country.

An export of any item or technology that was created in the country in which you work may occur by sending, taking, or transmitting goods, software, services or technology across any national boundary or by disclosing technology to a person who is not a citizen of the country in which you work. Information for the design, development, production or use of any product is defined as technology and includes design specifications, instructions, skills training, working knowledge and consulting services. Consult with the Office of Export/Import Compliance, Legal Affairs, or the Office of Ethics and Compliance whenever questions on this subject arise.

For more information on this topic, see the Export/Import Laws Policy.

Export/import controls is a complex legal area with a host of regulatory requirements. Please consult with appropriate EDS personnel if you have any doubts about whether a conversation or exchange may be an export.

Q: ***I am a software engineer located in the United States, and I sometimes deal with clients in other countries. Are all of my conversations with clients outside the U.S. "exports" of technology?***

A: ***Your conversations with clients in or from other countries may constitute "exports," depending on what the conversation concerns. You should consult the Export/Import Laws Policy for detailed information, and consult Legal Affairs, the Office of Export/Import Compliance, or the Office of Ethics and Compliance when specific questions arise.***

International Boycotts

U.S. anti-boycott laws apply to economic boycotts of other countries that are not sanctioned by the U.S. These laws require U.S. companies and all their controlled subsidiaries to report most requests to support an unsanctioned boycott, whether the requests are oral or in writing. So that EDS can comply with these laws, you must report any suspicious requests or contract terms to the Office of Export/Import Compliance and Legal Affairs even if you do not intend to comply with the request.

Examples of boycott requests we generally cannot comply with and must report:

- Certify the goods are not from a particular country.
- Certify EDS does not have an office in a particular country.
- Identify the race, religion and sex of all employees who will work on this project.

Q: ***How do I know if I am being asked to engage in illegal boycott activity?***

A: ***In attempting to identify boycott-related requests or restrictions, pay particular attention to requests for information or contract terms that require:***

- ***Information about a person's past, present or prospective relationship with what the other party might refer to as "boycotted countries" or "blacklisted companies";***
- ***Information about a person's race, religion, gender or national origin; or***
- ***Discrimination against individuals or companies on the basis of race, religion, gender or national origin.***

In recent times the Arab League boycott of Israel has been the primary boycott that leads to companies being prosecuted for participating in an unsanctioned boycott.

U.S. Embargoes and Restricted or Denied Parties

Currently, the U.S. and its allies maintain embargoes against a number of countries. In addition, the U.S. also prohibits commercial activities with parties that have violated the U.S. export laws or that have been specially designated as having intentions harmful to the U.S. EDS complies with applicable U.S. laws regarding these embargoes and with the restrictions against doing business with any prohibited party. Always screen the names of clients, suppliers or subcontractors by selecting the Denied Parties List from the "Quick Links" drop-down menu on the Export Compliance Web site.

See the Defense Trade Controls-Embargo Reference Chart for a list of countries who are also restricted from receiving defense articles and services. Consult the Office of Export/Import Compliance or Legal Affairs if there are any questions about EDS' ability or the ability of EDS subsidiaries to do business involving a particular country or party.

When required by law, we must abide by embargoes and sanctions maintained by the U.S. and its allies.

Q: ***I would like to send some products to a potential client in a country that is subject to a U.S. embargo. Would it be okay if I send the products to a company outside the U.S. and that company then sends them on to the potential client?***

A: ***No. It is illegal to try to "get around" the embargo laws or to attempt to accomplish indirectly or through third parties what the embargo laws prohibit us from doing directly.***

Fair Competition

Antitrust laws and trade regulations are designed to encourage healthy competition in a fair and reasonable business climate. Most antitrust laws and trade regulations apply to both the marketing of products and the marketing of services.

Generally, antitrust laws prohibit any activity that may improperly reduce or inhibit competition. We compete vigorously and fairly in the conduct of business matters and always in compliance with applicable antitrust laws. Some of the most serious antitrust offenses are agreements between competitors that limit independent judgment and restrain trade, such as agreements to fix prices, restrict output or control the quality of products, or to divide a market for clients, territories, products or purchases. You should not agree with any competitor on any of these topics as these agreements are virtually always unlawful.

EDS must comply with all applicable competition laws. If you become aware of a conflict between U.S. laws and the laws of other nations, consult Legal Affairs.

Because of the complexity of antitrust laws, you must seek advice from Legal Affairs on any question regarding them. The penalties for violating antitrust laws and trade regulations can be extremely severe for both EDS and the individuals involved.

For more information on this topic, refer to the Antitrust Policy.

Q: ***A neighbor works for one of EDS' competitors. We have a friendly relationship, and last Sunday my neighbor asked me about pricing for one of our projects. I avoided the issue, but I'd like some guidance in case it happens again.***

A: ***You must absolutely avoid talking about pricing with any of EDS' competitors. While we understand that, in social situations, it can sometimes be difficult to act appropriately, you need to explain to your friend that EDS' policy strictly prohibits you from talking about price or other terms of sale with competitors.***

EDS depends on its reputation for honesty and integrity. The way we deal with our clients, competitors and suppliers molds our reputation, builds long-term trust and ultimately determines our success. We compete vigorously but fairly, and always play by the rules.

Compliance/Discipline

We are each responsible for reporting known and suspected violations of EDS policy or legal requirements. EDS takes all reports seriously and expects employees to be truthful and cooperate fully with investigations. Each report is reviewed and, if substantiated, resolved through appropriate corrective and/or disciplinary action, which may include verbal reprimand, written reprimand or termination of employment. Subject to applicable law, EDS will consider disciplinary action under appropriate circumstances, including circumstances where someone:

- Has authorized, condoned, participated in or concealed actions that violate these standards;
- Approves or disregards a violation, or through lack of diligence in supervision fails to prevent or report violations;
- Retaliates directly or indirectly or encourages others to retaliate for reported violations made in good faith; or
- Is uncooperative or untruthful during an investigation into any suspected violation of this Code, any EDS policy or legal requirement.

As part of EDS' procedure for receiving and handling complaints or concerns, EDS has established procedures for:

- The receipt, retention and treatment of complaints regarding accounting, internal accounting controls, or auditing matters; and
- The confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

Such procedures are set forth in EDS' Financial Integrity Policy and at EDS' corporate Web site.

If you know it's wrong, don't do it. If you see something that seems wrong, report it.

Q: ***What if my leader asks me to do something that is illegal?***

A: ***Don't do it! If you know or have a good faith reason to believe that it would be illegal or violate company policy, you should refuse to do it and report the matter to your leader's leader, Legal Affairs, the Office of Ethics and Compliance, or the Ethics Helpline.***

Substantive Changes to and Waivers of the Code of Business Conduct

Any waiver of the Code of Business Conduct for any director or executive officer must be made by EDS' full Board of Directors or a designated committee of independent directors as required by law or stock exchange regulation. Substantive changes and waivers of the Code for directors and executive officers will be promptly disclosed as required by law or stock exchange regulation.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS for any specific period or under specific terms and conditions. Unless contrary to applicable law or the terms of a written contract executed by an appropriate officer of EDS, employment at EDS is for no definite period and may be terminated at any time by the company or by an employee for any reason or for no reason at all and with or without notice. EDS, however, cannot and will not terminate employees for any unlawful reason.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time, without advance notice.

Director's Addendum to the EDS Code of Business Conduct

EDS Directors play a special role in the governance and conduct of EDS' business and affairs. In many cases, the duties and responsibilities and, therefore, the ethical obligations of non-employee (outside) directors are the same as or comparable to those of employees. Non-employee directors should adhere to the Code (including those provisions relating to conflicts of interest, corporate opportunities, confidentiality, fair competition, protection and proper use of EDS assets, and compliance with laws and regulations) in carrying out their duties on behalf of EDS to the extent and in a manner consistent with their special duties and obligations. Because outside directors are not employees of EDS, they are not and should not be subject in all respects to specific portions of the Code. Non-employee directors of EDS, for example, are not expected to obtain approval of any EDS leader before accepting employment with another company.

The conduct of both employee and non-employee directors is, in some cases, governed by additional principles to which employees are appropriately not subject, such as those contained in EDS' Corporate Governance Guidelines. For example, directors are expected to comply with the provisions of those guidelines before accepting service on another board of directors.

Directors should (a) ethically handle situations that could give rise to a conflict of interest including the appearance of a conflict, (b) fully and promptly disclose any conflict of interest to the General Counsel as set forth in this Code, and (c) take appropriate preventative or corrective actions (e.g., recusal from certain decisions), as determined by the Board or a designated committee.

Code of Business Conduct Certification

By signing below, I hereby acknowledge that I am aware of the EDS Code of Business Conduct, have access to it, and have read and understand it. I am also aware of how to seek guidance and report violations.

Printed Name:_____

Signature:_____

Date:_____

EDS NetID:_____ Keyword: certify

All employees and directors of EDS companies (except where the local law does not permit) are required to certify annually (new employees within thirty (30) days of hire). You can certify at http://ethicscertification.eds.com (preferred), or if EDS intranet connectivity is unavailable, by submitting a hard copy to your leader.

If an employee provides a hard copy, the manual certification is to be retained in the employee's employment file for the duration of his/her employment with EDS and for a minimum of five (5) years (or as required by more stringent applicable law) following the individual's separation from EDS employment. Upon receiving the manual certification form from the employee, the leader is to electronically certify on behalf of the employee at: http://cobc.legalaffairs.eds.com.

Other Country Code Provisions

EDS operates in many countries and many cultures. We respect the laws and regulations of all of the places where we do business. Laws can sometimes differ and even conflict. If there is a conflict between applicable laws or between applicable law and a policy set forth in this Code, you should consult with Legal Affairs before taking any action. The following sections discuss certain provisions of laws of some of the places where EDS does business.

Canadian Code Provisions

Outside Employment

Because EDS has clients, suppliers and other business relationships in different industries and settings, outside employment may create or appear to create a conflict of interest. As a result, and subject to applicable legislation, before accepting employment in addition to your role at EDS, any potential conflict of interest must be reviewed with your EDS leader and approved by that leader before accepting the additional job.

In accepting outside employment, remember your commitment to EDS. You should not use EDS time or resources to benefit the outside employer, and the employment should not adversely affect your judgment, decisions or ability to meet EDS work-assignment responsibilities.

Psychological Harassment and Bullying

EDS Canada prohibits psychological harassment and bullying in the workplace, which include repeated and hostile or unwanted conduct, verbal comments, actions or gestures that affect an employee's dignity or psychological or physical integrity, and that result in a harmful work environment for the employee. EDS expects employees to report such behaviour and leaders to promptly act upon such allegations. If an investigation confirms improper conduct occurred, EDS will take appropriate action.

Application of Laws in the International Arena

Canadian law may govern our practices outside Canada. If you are uncertain, check with the Canadian office of EDS Legal Affairs or your EDS Human Resources representative about Canadian and/or foreign laws that affect your activities abroad.

For example, Canadian law prohibits (1) bribery, (2) export of some goods and technologies without a permit, (3) participating in international boycotts, and (4) trade with certain embargoed countries.

Bribery and Improper Payments

Within Canada, governments seek to prevent and prohibit potential domestic corruption by a combination of statutes, parliamentary rules and administrative provisions. The Criminal Code includes offences that prohibit bribery, frauds on the government and influence peddling, fraud or breach of trust in connection with duties of office, municipal corruption, selling or purchasing offices, influencing or negotiating appointments or dealing in offices, possession of property or proceeds obtained by crime, fraud, laundering proceeds of crime, and secret commissions.

Internationally, Canada has actively participated in anticorruption initiatives in various international forums. In response to these initiatives, the Corruption of Foreign Public Officials Act features the offence of bribing a foreign public official. The offence of bribing a foreign public official is added to the list of offences found in the Income Tax Act to deny claiming bribe payments as a deduction. Amendments to the Criminal Code enable the prosecution of possession and laundering offences in respect of the offences of bribing foreign public officials, conspiracy or an attempt to commit the offence, as well as aiding and abetting and counseling others to commit the offences.

Beyond compliance with these laws, each employee is expected to avoid conduct that could appear to violate the law. Therefore, according to EDS policy, we should not make any payments or give gifts related to EDS business activities to officials of Canada or other countries unless the transactions are first approved by the Canadian office of EDS Legal Affairs.

Export/Import Control Regulations

EDS conducts its international business in strict compliance with Canadian export/import laws and regulations. Under regulations administered by the Minister of Foreign Affairs, Export and Import Controls Bureau, the export of goods, software, services or technology from Canada may require export permits.

Exports may occur by sending, taking, or transmitting goods, software, services or technology out of Canada. Because Canada is party to a number of international regimes related to the control of the export of "strategic goods," and controls have been implemented to comply with Canada's multilateral commitments, consult with the Canadian office of EDS Legal Affairs whenever the question of export arises.

International Boycotts

It is an offence under the Foreign Extraterritorial Measures Act to comply with a foreign state's or tribunal's international trade or commerce policy that adversely affects or may adversely affect Canadian interests in relation to international trade or commerce, or that infringes Canadian sovereignty. All requests and contract terms that purport to have EDS comply with the trade restrictions or embargoes ordered by a foreign government or its agencies must be reported to the Director of the Canadian office of EDS Legal Affairs, who will take appropriate action.

Embargoes

Currently, Canada maintains commercial embargoes against a number of countries. EDS complies with applicable Canadian laws regarding these embargoes. Because the list of embargoed goods and countries maintained by the Minister of Foreign Affairs changes frequently, consult with the EDS Canadian Export Compliance Coordinator 416 814 1543 if you have any questions about EDS' ability to do business with a particular country.

Fair Competition

Fair competition laws and trade regulations are designed to encourage healthy competition in a fair and reasonable business climate. To provide clients with the best combination of price and quality, and to promote efficiency, companies that do business in Canada must comply with competition legislation.

In Canada, fair competition is governed primarily by the Competition Act, which was enacted to ensure the preservation and protection of free competition and to prevent artificial restraints on Canada's economic system. Individuals, such as EDS employees, must not enter into formal or informal arrangements (expressed or implied) with any competitor that set prices, costs, terms or conditions of sales or services; that assign clients, markets, territories, services, or product plans; or that deal with any other competitively sensitive or non-public information. The Competition Act also states that sellers cannot lessen competition by discriminating in price between the purchasers of commodities of like grade, quality, and quantity, and buyers cannot knowingly purchase commodities in such anticompetitive circumstances. Further, it is prohibited for a seller to pay a commission or to allow other compensation to get around this prohibition.

Most other countries where EDS does business also have laws restricting attempts to monopolise or control competition. It is EDS' obligation to comply with these laws where they are applicable. Conflicts between Canadian competition and trade laws and the laws of other nations will be addressed by the Canadian office of EDS Legal Affairs.

EDS' responsibility as a global corporate citizen requires compliance with these laws. Failure to comply will not be excused by the belief that the act was in the "corporate interest" or that it was "pursuant to instructions" from other people within the organisation. Beyond compliance, each employee is expected to avoid conduct that could appear to violate the law.

Because of the complexity of competition laws, it is imperative to seek advice from the Canadian office of EDS Legal Affairs on any question regarding them. The penalties for violating competition laws and trade regulations can be extremely severe for both EDS and the individuals involved.

Private Sector Personal Information Protection Legislation in Canada

In addition to complying with the Global Privacy and Data Protection policy, EDS in Canada conducts its business in compliance with applicable statutes and regulations regarding protection of personal information. In Canada EDS has implemented, and monitors on a regular basis for changes, a comprehensive program to observe Quebec's An Act respecting the Protection of Personal Information in the Private Sector, B.C.'s Personal Information Protection Act, Alberta's Personal Information Protection Act, and the Personal Information Protection and Electronic Documents Act, each as such legislation applies to EDS with respect to personal information of its employees. This includes disclosing the purpose for which the information is collected and/or being shared with third parties, seeking consent if it is to be used for another purpose, retention for the statutory time periods, a mechanism to review and to correct (and if necessary register a complaint with the EDS Canada Privacy Officer) the personal information about the employee held by EDS.

EDS Canada's Personal Information Protection Policy is available to view in the Human Resources Section of the infoCanada Web site.

Substance Abuse Policy

The testing provisions of the Substance Abuse Policy do not apply to EDS Canada.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time without advance notice.

If you require clarification regarding a policy in Canada, please refer to the infoCanada site under Human Resources.

Code of Business Conduct Certification

If an employee provides a hard copy of the Manual Certification Form, the form is to be retained in the employee's employment file for the duration of his/her employment with EDS and for a minimum of one (1) year (or as required by more stringent applicable law) following the individual's separation from EDS employment. Upon receiving the manual Code certification form from the employee, the leader is to electronically certify on behalf of the employee at: http://cobc.legalaffairs.eds.com.

United Kingdom Code Provisions

Outside Employment

Because EDS has clients in many different industries and has many suppliers and business relationships, outside employment may create or appear to create a conflict of interest. As a result, and subject to applicable legislation, before accepting employment in addition to your role at EDS, any potential relationship or employment must be reviewed with your EDS leader and approved by the leader before accepting the additional job.

In accepting outside employment, remember your commitment to EDS. You should not use EDS time or resources to benefit the outside employer, and the employment should not adversely affect your judgment, decisions or ability to meet EDS work-assignment responsibilities.

Personal Privacy/Data Protection

Employee privacy can become an issue when personal use is made of EDS resources. Although EDS assets are intended for use in supporting and conducting EDS business, limited and reasonable personal use is permitted. (See the section titled "Proper Use of Corporate Assets and Resources" contained in this Code.) EDS reserves the right to monitor the use and contents of its assets and resources in accordance with applicable legislation. This will include employees, contract laborers and others using EDS' and its clients' facilities. Examples of such monitoring may include interception of e-mails, monitoring Internet access, monitoring telephone calls, monitoring of use of swipe cards, monitoring use of EDS and client computer facilities and systems, and recording activity with CCTV cameras for the purpose of employee safety and security of premises. Monitoring complies with employment contracts and policies and proper business practices.

If EDS is required to disclose data held on its electronic communications systems and networks, information such as employee password protection may be requested and must be provided to EDS.

Where appropriate and in accordance with applicable legislation, EDS reserves the right to pass on information and data obtained in the course of monitoring referred to above to the subject's leader or employer.

For more information on this topic, see the Use of Corporate Assets Policy, the Global Privacy and Data Protection Policy, the Financial Integrity Policy, the Security Policy, the Information Handling Security Policy, Enterprise Security Policies & Standards (ESPS), UK Electronic Communications Policy and the section of the Code titled "Computers and Equipment, Network Security, Photographic and Audio Devices."

Solicitation/Distribution

In the interest of a professional work environment and to protect EDS employees and directors from unwanted solicitation, you may not solicit or distribute any nonwork-related literature for any purpose during your working time or the working time of the person(s) you are soliciting. You may not distribute literature at any time in any working area. Selling, trading, or bartering of services or merchandise to others, as well as conducting personal business, is prohibited on EDS premises, except for company-endorsed activities. Participating in or soliciting for organised or commercial lotteries or other gaming or gambling activities is prohibited, except as permitted below.

Persons who are not employees may not solicit or distribute literature for any purpose on EDS premises at any time, unless they have the approval of the senior leader of the business or support organization, as designated in the EDS Organization Chart published on infoCentre.

In the UK, this section of the Code does not prevent employees from participating in the national lottery or undertaking other gaming or gambling activities so long as such activity does not occur during an employee's working time and does not bring EDS into disrepute.

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in the UK.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Where reference is made to the EDS Disciplinary Procedure, this will be the EDS UK Disciplinary Procedure in place. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time without advance notice.

Australian Code Provisions

Drugs and Alcohol

The Substance Abuse policy applies; however, it is not the practice to apply the Enforcement/Testing process to EDS employees in Australia.

Danish Code Provisions

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in Denmark.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Where reference is made to the EDS Disciplinary Procedure, this will be the EDS Denmark Disciplinary Procedure in place. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time without advance notice.

Irish Code Provisions

Personal Privacy/Data Protection

Employee privacy also becomes an issue when personal use is made of EDS resources. Although EDS assets are intended for use in supporting and conducting EDS business, limited and reasonable personal use of company equipment and systems is permitted. (See the section titled "Proper Use of Corporate Assets and Resources" contained in this Code). Where not prohibited by law or regulation, EDS reserves the right to monitor the use and contents of its assets and resources. We should have no expectation of privacy when using EDS resources, whether for business or personal use. EDS may inspect the corporation's facilities, property, records and systems, including electronic systems, and inspect the information contained in them with or without advance notice to employees – even when information is stored under an individual's personal identification code or password. EDS employees will be made aware where such monitoring may take place.

For more information on this topic, see the Use of Corporate Assets Policy, the Global Privacy and Data Protection Policy, the Financial Integrity Policy, the Security Policy, the Information Handling Security Policy, Enterprise Security Policies & Standards (ESPS), and the section of the Code titled "Computers and Equipment, Network Security, Photographic and Audio Devices."

Sexual Harassment and Other Unlawful Behaviour

EDS does not tolerate sexual harassment or other unlawful behaviour in the workplace, whether committed by a co-worker, leader, client, contract laborer, supplier or anyone else. Actions, words, jokes or comments that are derogatory and based on any person's gender, race, age, sexual orientation, gender identity, religion, disability, family status, marital status or Membership of the Traveller community will not be tolerated at EDS. Although sexual harassment appears in various forms and degrees, it generally consists of unwelcome sexual advances, unwelcome requests for sexual favours or other unwelcome verbal or physical conduct of a sexual nature. Sexual harassment occurs when submission to or rejection of sexual advances adversely affects your employment in any way (for example promotion, termination or unfavourable work assignments) or when unwelcome sexual conduct otherwise interferes with your job performance or creates an intimidating or hostile work environment.

Solicitation/Distribution

In the interests of a professional work environment and to protect EDS employees and directors from unwanted solicitations, unless specifically preapproved by the senior leader of the business or support organisation, as designated in the EDS Organization Chart published on infoCentre, employees may not (1) solicit or distribute any nonwork-related literature for any purpose; (2) sell, trade or barter services or merchandise to others; or (3) conduct a personal business on EDS premises. Soliciting for organised or commercial lotteries or other gaming or gambling activities is prohibited.

Persons who are not employees may not distribute literature or solicit for any purpose on EDS premises at any time, unless they have the approval of the senior leader of the business or support organisation, as designated in the EDS Organization Chart published on infoCentre.

Drugs & Alcohol: Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in Ireland.

Outside Employment

Because EDS has clients, suppliers and other business relationships in different industries and settings, outside employment may create or appear to create a conflict of interest. As a result, and subject to applicable legislation, before accepting employment in addition to your role at EDS, any potential relationship or employment must be reviewed with your EDS leader and approved by that leader before accepting the additional job.

In accepting outside employment, remember your commitment to EDS. You should not use EDS time or resources to benefit the outside employer, and the employment should not adversely affect your judgment decisions or ability to meet EDS work-assignment responsibilities.

Document Retention

Laws, regulations and EDS guidelines require retention of certain records for various periods of time. When litigation or an investigation is pending, relevant records must not be destroyed. If EDS receives a subpoena or Order to produce records, EDS may not in any way modify these records. Such records include, but are not limited to, personnel files, working time records and electronic records.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Where reference is made to the EDS Disciplinary Procedure, this will be the EDS Irish Disciplinary Procedure in place. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract, and EDS retains the right to unilaterally modify this Code at any time, without advance notice.

New Zealand Code Provisions

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in New Zealand.

Norwegian Code Provisions

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in Norway.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Where reference is made to the EDS Disciplinary Procedure, this will be the EDS Norway Disciplinary Procedure in place. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time without advance notice.

Swedish Code Provisions

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in Sweden.

No Rights Created

Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

Any changes, modifications will be handled in compliance with the Swedish Act on Co-determination at Work (MBL), although EDS retains the right to unilaterally modify this Code at any time without advance notice.

In the event of need for corrective or disciplinary action, EDS Sweden will act in compliance with Swedish legislation and collective agreements.

Belgian Code Provisions

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in Belgium except as permitted by, and in accordance with, applicable Belgian labor and employment laws.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Where reference is made to the EDS Disciplinary Procedure, this will be the EDS Belgium Disciplinary Procedure in place. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time without advance notice.

Dutch Code Provisions

Substance Abuse, Enforcement Testing

The principles and policy of maintaining a drug-free workplace will apply, but the Enforcement/Testing process will not apply to EDS employees in The Netherlands.

No Rights Created

The EDS Code of Business Conduct is not intended to confer any special rights or privileges upon specific individuals, provide greater or lesser rights under applicable law or entitle any person to remain employed by EDS. Unless contrary to the terms of a written contract executed by an authorised representative of EDS, employment at EDS may be terminated by the company in accordance with applicable law, or by an employee with or without cause in accordance with applicable law and/or the terms of a written contract with the company. Where reference is made to the EDS Disciplinary Procedure, this will be the EDS Dutch Disciplinary Procedure in place. Although some of the guidelines set forth herein may suggest, even strongly, that certain procedures or steps be followed, these procedures should not be interpreted as altering the terms of employment and do not constitute an employment contract.

The EDS Code of Business Conduct is not a contract. EDS retains the right to unilaterally modify this Code at any time without advance notice.

Contact List

Organization	Contact
Chief Security & Privacy Office *Keyword: security*	CSPO contacts
Community Affairs *Keyword: community affairs*	Community Affairs contacts
Corporate Audit *Keyword: audit*	1 972 605 3600 [8 835]
Corporate Public Relations	Corporate Public Relations Contacts
Corporate Records Center	1 972 277 4100
Employee Relations Offices Herndon, VA Plano, TX *Keyword: employee relations*	 1 703 742 1400 [8 432] 1 972 605 3480 [8 835]
Ethics and Compliance Helpline	1 888 EDS ETHK (888 337 3845) (no caller ID on this line)
Government Liaison and Compliance Hotline (U.S.)	1 703 742 2744 [8 432]
Government Liaison and Compliance Office (U.S.)	1 703 742 2268 [8 432]
Human Resources *Keyword: HR*	HR Contacts
Legal Affairs Asia Pacific Canada Europe (EMEA) Latin America United States *Keyword: legal affairs*	 61 2 8965 0717 1 416 814 4907 44 20 7569 5108 1 972 605 5500 [8 835] 1 972 605 5500 [8 835]
Office of Ethics and Compliance *Keyword: ethics*	1 972 605 5607
Office of Export/Import Compliance *Keyword: export*	1 314 264 8833 44 07790 493150
Supply Chain Management Helpdesk *Keyword: supply chain*	1 866 740 3978

SCHEDULE 40

JSRFP

See the attached

BRITISH COLUMBIA
The Best Place on Earth

June 19, 2007

To All Proponents

On behalf of the Ministry of Labour and Citizens' Services, it is my pleasure to issue this Joint Solution Procurement Request for Proposal for the Strategic Transformation and Mainframe Services Project.

Workplace Technology Services is the information technology division of the Ministry of Labour and Citizens' Services. As the steward of information technology services, assets, and supply arrangements, Workplace Technology Services is responsible for providing cost effective management and supply of information technology services to core government ministries, program managers and government employees. The division is also responsible for understanding the business objectives, future directions, and unique requirements of the programs it supports.

The Strategic Transformation and Mainframe Services Project, led by Workplace Hosting Services, a branch of Workplace Technology Services, is an important initiative that seeks to address three key areas: the provision of mainframe services, the examination of transformational opportunities related to the current hosting services delivery model (including processes, capabilities and the services provided to its public sector clients), and the provision of data center facility services.

Through this collaborative Joint Solution Procurement process, we intend to select a Service Provider to work over the longer term with the Ministry to assist in transforming Workplace Hosting Services into a world class service delivery organization, providing services that are responsive and flexible to the evolving needs of government and will ensure the ongoing reliable and secure delivery of technology services. By combining the strengths, experiences and capabilities of both the public and private sectors, we will achieve the best possible solution for government.

I look forward to your proposals and thank you in advance for your participation and contribution to this significant project.

Sincerely,

[Original signed by]

Lori Wanamaker, CA
Deputy Minister

Deputy Minister
Ministry of Labour and Citizens' Services

Office of the Deputy Minister

Mailing Address:
PO Box 9440, Stn Prov Govt
Victoria BC V8W 9V3

BRITISH COLUMBIA
The Best Place on Earth

Ministry of Labour and Citizens' Services

Joint Solution Procurement
for the
Strategic Transformation and Mainframe Services Project

Government Contact:

All enquiries related to this Joint Solution Request for Proposal, **JSRFP# SATP - 231** are to be directed in writing to the person set forth below, who will respond to all enquiries if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all Proponents at the Province's option.

Pelle Agerup
Director, Project Procurement, Strategic Acquisitions
Common Business Services, Shared Services BC
Email: pcadmin@gov.bc.ca
Facsimile: (250) 356-0846

Delivery of Proposals:

Proponents should deliver ten (10) complete hard-copies **and** one electronic copy on CD of their Proposal. Proposals and their envelopes should be clearly marked with the name and address of the Proponent, the JSRFP number, and the project title. Proposals must be delivered by hand or courier (not be sent by mail, facsimile or email) prior to: **2:00 pm, Pacific Time on, July 26, 2007 at:**

Ministry of Labour and Citizens' Services
Strategic Acquisitions and Technology Procurement Branch
c/o Reception Desk
2nd Floor, 563 Superior Street
Victoria, British Columbia, V8V 1T7
Attention: Pelle Agerup

Proponent Meeting

A Proponent Meeting will be held on June 25, 2007 at St Ann's Academy, The auditorium, 835 Humboldt Street, Victoria, British Columbia at 11:00 AM, Pacific Time. Proponents planning to attend should email the Government Contact above, stating the number of attendees.

Please note that this meeting is intended to provide further information and address questions regarding the Strategic Transformation and Mainframe Services Project. Dial-in access may be provided. Instruction on how to dial-in can be requested in advance from the Government Contact above; however, audio quality cannot be assured. Attendance is optional and minutes will be taken. A copy of the recorded minutes and a list of attendees may be posted as an Addendum to this JSRFP on BC Bid.

TABLE OF CONTENTS

TABLE OF FIGURES

1 JOINT SOLUTION REQUEST FOR PROPOSAL INTRODUCTION

1.1 EXECUTIVE SUMMARY

The Ministry is interested in receiving Proposals from qualified and experienced Proponents in formulating and delivering hosting services, data centre facility services and strategic transformation services related to large corporate hosting infrastructure. The eventual Service Provider will be expected to assume responsibility of Workplace Technology Services' (WTS) hosting (including mainframe) services, provide data centre facility services, and through an evolving transformation strategy, provide an integrated Solution that will enable WTS to deliver world class services to its clients in the public sector.

The purpose of this Joint Solution Request for Proposal (JSRFP) is to identify Proponents with the optimum combination of capacity, capability and commitment to work with the Ministry and propose a Concept that will form the basis of a jointly created Solution to achieve the best business outcomes for the STMS Project.

The term of the Final Contract is anticipated to be up to fifteen years with options by the Province for extension of up to five years.

1.2 THE JSP PROCESS

The Ministry has opted to use the Joint Solution Procurement (JSP) Process (which is a multi-stage procurement process for complex, long-term initiatives) in order to identify and joint solution with Proponents an optimal Solution that meets the vision and objectives described in section 3. The four phases of the JSP Process are outlined in Figure 1 below:

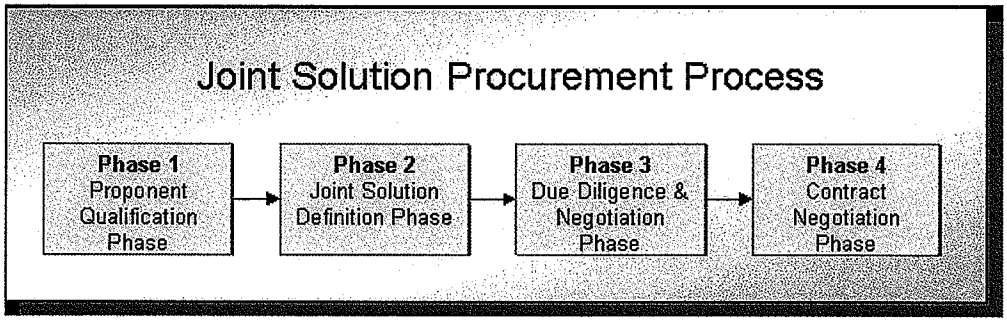


Figure 1 – Joint Solution Procurement Process

The first phase of the JSP Process (Proponent Qualification Phase) is designed to qualify and short-list Proponents primarily on their capacity, capability and commitment to be the Service Provider to the Ministry for the STMS Project. The Ministry will also be seeking from Proponents a Concept that describes, at a high-level, the Proponents approach to meet the STMS Project requirements as set out in this JSRFP.

Following the Proponent Qualification Phase, two Preferred Proponents will be selected and invited to enter into the second phase of the JSP Process, the Joint Solution Definition Phase. The Joint Solution Definition Phase allows for the joint development of proposed Solutions in an iterative approach that will maximize the business objectives of both parties. The form of the deal structure will depend on the outcome of the Joint Solution Definition Phase.

Ultimately, the Successful Proponent will be invited by the Province to advance to the third phase, the Due Diligence & Negotiation Phase, and the fourth phase, the Contract Negotiation Phase, with the intent to enter into a Final Contract.

This Space Intentionally Left Blank

1.3 DEFINITIONS AND ADMINISTRATIVE REQUIREMENTS

1.3.1 Definitions

Throughout this JSP Process, the following definitions will apply:

a) "Broader Public Sector" or "BPS" includes crown corporations and agencies that are owned or controlled directly or indirectly by the Province, and all other levels of government within British Columbia including, without limitation, all municipalities, cities, towns, counties or other political jurisdictions of British Columbia, and any agency, board, council, department, authority, tribunal or commission of the Province or of any of the foregoing, and all universities, colleges, schools, school boards, hospitals and health authorities in British Columbia;

b) "Concept" means the high level concept relating to the Scope of the Opportunity that is presented orally and in writing by a Proponent to the Province during Stage 3 of the Proponent Qualification Phase;

c) "Contract Negotiation Phase" means phase 4 of this JSP Process which commences upon the Province indicating that it is prepared to start negotiation of the Final Contract with the Successful Proponent and ends upon the execution of the Final Contract;

d) "Current Data Centre Facilities" means the facilities that WTS currently uses to deliver its Current Hosting Services as more particularly described in section 2.3.1.4;

e) "Current Hosting Services" means the services provided by Workplace Hosting Services described in section 2.3.1.3;

f) "Due Diligence & Negotiation Phase" means phase 3 of this JSP Process which commences upon an invitation being extended by the Province to the Successful Proponent to enter into phase 3 of this JSP Process and ends upon the Province indicating that it is prepared to start negotiation of the Final Contract with the Successful Proponent;

g) "Final Contract" means the written agreement executed by the Province and the Successful Proponent resulting from completion of the Contract Negotiation Phase, as more particularly described in section 1.3.7;

h) "Information Control Office" means the JSP Process information management control structure that is established to control the flow of information between the Ministry and Preferred Proponents during the Joint Solution Definition Phase and subsequent phases of the JSP Process;

i) "Intellectual Property" means any and all patents, trade-marks, trade, business or domain names, copyright, rights in concepts, inventions, know how, trade secrets and all other intellectual property rights which may now or in the future exist;

j) "Joint Solution Definition Agreement" or "JSDA" means the agreement that will be entered into by the Province and each Preferred Proponent prior to the Joint Solution Definition Phase which will include the provisions described in Appendix C;

k) "Joint Solution Definition Phase" or "JSD Phase" means phase 2 of this JSP Process which commences upon invitations being extended to Preferred Proponents to enter into phase 2 of this JSP Process and ends upon an invitation being extended by the Province to one of the Preferred Proponents to become the Successful Proponent;

l) "JSP Process" means the Joint Solution Procurement Process for the STMS Project;

m) "JSRFP" means this joint solution request for proposal document and any amendments to it;

n) "Letter of Intent" means the letter of intent that will be entered into by the Successful Proponent prior to the Due Diligence & Negotiation Phase;

o) "Ministry" means the Province's Ministry of Labour and Citizens' Services or any such successor organization that is responsible for the STMS Project;

p) "must" or "mandatory" in respect of section 1.3 Definitions and Administrative Requirements and section 5.6.1.1, means a requirement that must be met in order for a Proposal to receive consideration;

q) "Potential In-Scope" means the scope defined in section 3.4.2;

r) "Preferred Proponents" means the Proponents who are invited by the Province to advance to the Joint Solution Definition Phase and who sign the Joint Solution Definition Agreement;

s) "Proponent" means the entity that submits, or intends to submit, a Proposal in response to this JSRFP, and where the Proposal consists of a joint submission or contemplates the use of Subcontractors, then the Proponent is the

lead entity or prime-contractor responsible for the Proposal;

t) "Proponent Qualification Phase" means phase 1 of this JSRFP which commences upon the release of this JSRFP and ends upon invitations being extended by the Province to Preferred Proponents to enter into the Joint Solution Definition Phase;

u) "Proposal" means the written submission required for Stage 1 of the Proponent Qualification Phase;

v) "Province" means Her Majesty the Queen in Right of the Province of British Columbia as represented by the Minister of Labour and Citizens' Services;

w) "Restricted Documents Room" means the documents room the Province may make available to short-listed Proponents as more particularly described in section 5.1.5;

x) "Scope of the Opportunity" means the STMS Project Scope and Potential In-Scope as more particularly described in section 3.4;

y) "Services" means the services that will be delivered over the term of the Final Contract;

z) "Service Provider" means the Successful Proponent who enters into the Final Contract with the Province;

aa) "should" or "desirable" in respect of section 1.3 Definitions and Administrative Requirements and the evaluation criteria means a requirement having a significant degree of importance to the objectives of the JSRFP;

bb) "Solution" means the solution and strategic transformation framework for STMS that is developed during the Joint Solution Definition Phase in response to the Ministry's business goals and desired outcomes for the STMS Project;

cc) "Stage 1" means the initial stage of the Proponent Qualification Phase during which Proposals will be created by Proponents and evaluated by the Province;

dd) "Stage 2" means the second stage of the Proponent Qualification Phase during which up to four Proponents will be asked to participate in separate Workshops with the Province and be provided with access to a Restricted Documents Room;

ee) "Stage 3" means the final stage of the Proponent Qualification Phase during which the Proponents who participated in the Workshops will present their Concepts to the Province, both orally and in writing;

ff) "STMS Project" or "Strategic Transformation and Mainframe Services Project" means the project described in this document, beginning with the JSP Process and continuing through the design, transition and ongoing operation of the Services during the term of the Final Contract;

gg) "STMS Project Scope" means the scope defined in section 3.4.1;

hh) "Subcontractors" mean entities that are included or intending to be included in a joint proposal with a Proponent or are retained by the Contractor to perform certain services in respect of the Final Contract;

ii) "Successful Proponent" means the Preferred Proponent who is invited by the Province to advance to the Due Diligence & Negotiation Phase and who signs a Letter of Intent;

jj) "Workplace Hosting Services" means the branch of the Ministry responsible for the STMS Project or any successor organization;

kk) "Workshops" means the working sessions between a Proponent and the Ministry during Stage 2, as more particularly described in section 5.1.6.; and

ll) "WTS" means the Workplace Technology Services division of the Ministry.

1.3.2 JSP Process

This JSP Process will consist of four (4) phases: the Proponent Qualification Phase, the Joint Solution Definition Phase, the Due Diligence & Negotiation Phase and the Contract Negotiation Phase.

1.3.3 Proponent Qualification Phase

1.3.3.1 Terms of the Proponent Qualification Phase

The following terms apply to the Proponent Qualification Phase of this JSRFP. In consideration of the Province's preparation of this JSRFP document, in conducting the JSRFP and the Proponents' opportunity to submit a Proposal, each Proponent hereby acknowledges and agrees by submitting a Proposal in response to this JSRFP that the Proponent is accepting and agreeing to be bound by the terms of this JSRFP. Provisions in a Proposal that conflict or are inconsistent with any of the terms of this JSRFP shall be of no force or effect.

1.3.3.2 Process of the Proponent Qualification Phase

The Proponent Qualification Phase will consist of three stages:

a) Stage 1 – During this stage Proponents will submit Proposals in accordance with the terms of this JSRFP. Each Proposal will be evaluated by the Province. The Province will

select up to four Proponents to advance to Stage 2 of the Proponent Qualification Phase based upon the Province's evaluation of the Proposals;

b) Stage 2 – During this stage Workshops will be held with up to four Proponents that have advanced from Stage 1. Subject to the terms of this JSRFP, each of the Proponents from Stage 2 will advance to Stage 3 of the Proponent Qualification Phase; and

c) Stage 3 - During this stage each of the Proponents who have advanced from Stage 2 will present their Concepts to the Province. The Province will initially select up to two Proponents who will become Preferred Proponents and will advance to the Joint Solution Definition Phase.

Neither the acceptance by the Province of any Proposal, the conducting of any Workshop nor the receipt by the Province of any Concept in any format whatsoever shall under any circumstances cause any express or implied commitment or undertaking on the part of the Province to advance any Proponent to the next stage or phase, to receive any presentation from a Proponent, to acquire services, to undertake any form of transaction or to continue the JSRFP process.

1.3.3.3 Receipt Confirmation Form

Proponents are advised to fill out and immediately return the Receipt Confirmation Form attached as Appendix B. Subsequent information may be posted by the Province on BC Bid or distributed via email to those who have returned a Receipt Confirmation Form.

Proponents who have returned the Receipt Confirmation Form may be notified that certain additional information is available. In order to obtain such information, the Proponents must also sign and return to the Province the confidentiality form which will be provided by the Province with the notification. Those Proponents who sign and return the confidentiality form will be provided a copy in accordance with the Proponents' Receipt Confirmation Form or, for viewing purposes only, in a secure location that may be established by the Province.

1.3.3.4 Enquiries

All enquiries related to this JSRFP are to be directed, in writing, to the person set forth below. Information about this JSRFP obtained from any other source is not official and should not be relied upon. Enquiries and responses will be recorded and may be distributed to all Proponents at the Province's option.

Pelle Agerup
E-mail: pcadmin@gov.bc.ca
Fax: (250) 356-0846

The Province has no obligation to ensure consistency between each of the Workshops or each of the Concept presentations. Accordingly, during Stages 2 and 3, questions and responses exchanged between the Province and one Proponent may differ from questions and responses exchanged between the Province and any other Proponent. The Province does not intend to share the questions or answers that are exchanged with a Proponent during Stages 2 and 3 with any other Proponents; however, if a Proponent makes a request for information during a Workshop that the Province determines to be a request for basic information that should be made available to all Proponents, then the Province, in its sole discretion, may distribute that basic information to all Proponents participating in the Workshops.

1.3.3.5 Closing Date and Time

Ten (10) complete hard copies of the Proposal and one electronic copy on CD should be submitted. Proposals must be delivered by hand or courier (not sent by mail, facsimile or email), and received prior to 2:00 PM, Pacific Time, on Thursday, July 26, 2007 at:

Ministry of Labour and Citizens' Services
Strategic Acquisitions and Technology Procurement Branch

c/o Reception Desk
2nd Floor, 563 Superior Street
Victoria, B.C., V8V 1T7
Attention: Pelle Agerup

Proposals and their envelopes should be clearly marked with the name and address of the Proponent, the JSRFP number, and the project title.

1.3.3.6 Late Proposals

Proposals will be marked with their receipt time at the closing location described in section 1.3.3.5. Late Proposals will not be accepted and will be returned to the Proponent. In the event of a dispute, the Proposal receipt time as recorded at the closing location will prevail whether accurate or not.

1.3.3.7 Signed Proposals

The Proposal must be signed by a person authorized to sign on behalf of the Proponent and will bind the Proponent to the terms of this JSRFP and any statements made in response to this JSRFP. The Proponent should ensure that its Proposal includes a letter or statement(s) substantially similar in content to the sample Proposal Covering Letter provided in Appendix A.

1.3.3.8 Changes to Proposals

By submission of a clear and detailed written notice, the Proponent may amend or withdraw its Proposal prior to the closing date and time. The Proponent cannot change the wording of its Proposal after

closing and no words or comments will be added to the Proposal after closing unless requested by the Province for purposes of clarification, or to correct minor defects pursuant to section 1.3.3.16 below.

1.3.3.9 Eligibility

A Proposal will not be evaluated if the Proponent's current or past corporate or other interests may, in the Province's opinion, give rise to a conflict of interest in connection with the STMS Project. Subcontracting to any firm or individual whose current or past corporate or other interests may, in the Province's opinion, give rise to a conflict of interest in connection with the STMS Project, will not be permitted. The Province may also remove a Proponent from any later stage of the Proponent Qualification Phase where the Province determines, in its opinion, that such Proponent's current or past corporate or other interests may give rise to a conflict of interest in connection with the STMS Project. Any such determination by the Province of a conflict of interest shall be final and shall be based upon such information as the Province in its sole discretion determines to be relevant.

1.3.3.10 Evaluation Committee

The evaluation of Proposals and Stage 3 Concepts will be undertaken by a committee formed by the Province which committee may include employees and contractors of the Province and other stakeholders and representatives of the Broader Public Sector. The evaluation committee may consult with such technical advisors, including financial, legal, operating, marketing, representatives of the Broader Public Sector and other experts, as the evaluation committee may, in its discretion, determine to be necessary. The evaluation committee may be expanded or its composition altered by the Province in its sole discretion during Stage 3.

1.3.3.11 Evaluation

The evaluation committee will check Proposals against the mandatory criteria. Proposals that do not meet all of the mandatory criteria will be rejected without further consideration. Proposals that do meet all of the mandatory criteria will also be evaluated against the desirable criteria. The Concepts will be evaluated against the criteria described in this JSRFP.

The Concepts will be evaluated against Stage 3 evaluation criteria. The Province will finalize the evaluation criteria for Stage 3 prior to opening of the Proposals and will distribute the finalized evaluation criteria to the short-listed Proponents.

1.3.3.12 Debriefing

At the conclusion of Stage 1, Proponents who are not invited to advance to Stages 2 and 3 of the Proponent Qualification Phase will be so notified in writing, and may then request a debriefing meeting with the Province. It is the intention of the Province to schedule these meetings after the Final Contract has been executed but the Province, in its discretion, may schedule these meetings sooner. Proponents who will not be invited to participate in the Joint Solution Definition Phase will be so notified in writing at the end of the Proponent Qualification Phase, and may then request a debriefing meeting, which will be scheduled by the Province following the execution of the Final Contract.

1.3.3.13 Proponent Expenses

Proponents are solely responsible for their own expenses in preparing a Proposal and for participating in any or all stages of the Proponent Qualification Phase including, without limitation, if the Province elects to reject all Proposals or to not ask any Proponents to advance to the Joint Solution Definition Phase. In no event will the Province or any of its employees, representatives or contractors be liable to any Proponent for any claims, whether for costs or damages incurred by the Proponent in preparing the Proposal, or in preparing for or participating in stages 1, 2 or 3, or any phase of this JSP Process, or for any loss of opportunity, loss of anticipated profit in connection with any Final Contract (whether or not the Final Contract is awarded to the Proponent or at all), or for any other loss, damage or claim of any kind whatsoever relating in any way to all or any portion of the JSRFP or the JSP Process.

1.3.3.14 Limitations of Damage

Further to the preceding paragraph, the Proponent, by submitting a Proposal, agrees that it will not claim for any loss, costs or damages, for whatever reason, relating to the Final Contract (whether or not the Final Contract is awarded to the Proponent or at all) or in respect of the Proponent's preparation for or participation in, or failure to be invited to participate in, any one or more stage or phase of this JSRFP or JSP Process. If, contrary to the terms of this JSRFP the Province should be held liable for any reason whatsoever (whether in contract or in tort) for any of the foregoing losses, costs or damages, then such losses, costs or damages shall not, in any circumstances, exceed an amount equivalent to the lesser of (a) reasonable costs incurred by the Proponent in preparing its Proposal; and (b) CDN$ 100,000.

1.3.3.15 Right of the Province to Check References

The Province reserves the right to verify a Proponent's references at any point in the JSP Process.

1.3.3.16 Correction of Minor Defects

The Province reserves the right, in its sole discretion, to correct minor defects in the Proposals or Concepts.

1.3.3.17 Acceptance of Proposals

This JSRFP should not be construed as an agreement to purchase goods or services. The Province is not bound to enter into any contract with any Proponent including, without limitation, any Proponent who submits the lowest priced Proposal or Concept. Proposals and Concepts will be assessed in light of the evaluation criteria described in this JSRFP. The Province will be under no obligation to receive further information, whether written, oral, or otherwise, from any Proponent at any stage in the Proponent Qualification Phase.

1.3.3.18 Restriction on Contact/No Lobbying

Proponents must not attempt to communicate directly or indirectly with any employee, contractor or representative of the Province, including the evaluation committee, during the Proponent Qualification Phase or discuss the STMS Project described in this JSRFP with members of the public, the press or the BPS, other than as expressly directed or permitted by the Province.

1.3.3.19 No Contract

By submission of a Proposal, Proponents agree that no Proponent will acquire any legal or equitable rights or privileges relative to the STMS Project described in this JSRFP prior to the full execution of a Final Contract. Further, the Province reserves the right not to enter into a Final Contract with any of the Proponents.

1.3.3.20 Liability for Errors

While the Province has used considerable effort to ensure the accurate representation of information in this JSRFP, and provided pursuant to this JSP Process, and such information is supplied solely as a guideline for Proponents. The Province does not warrant or guarantee the accuracy of such information, nor is such information necessarily comprehensive or exhaustive. Nothing in this JSRFP is intended to relieve Proponents from the obligation to form their own opinions and reach their own conclusions with respect to the matters addressed in this JSRFP.

1.3.3.21 Modification of Process or Project

The Province reserves the right to modify the JSP Process, this JSRFP or the STMS Project at any time in its sole discretion. This includes, but is not limited to, the right to cancel this JSRFP at any time, to extend the closing time, change the number of Proponents asked to advance to any stage of this JSRFP or any phase of this JSP Process, re-commence a stage or phase of this JSRFP or JSP Process, alter the STMS Project requirements or make other changes to the process or to a term set out in this JSRFP. If a modification is communicated to the Proponents prior to closing time, it is the Proponents' sole responsibility to ensure that they make appropriate use of that information.

1.3.3.22 Ownership of Proposals

Subject to the qualifications otherwise set out herein, all Proposals and Concepts will be received and, to the extent reasonably possible, held in confidence by the Province and the Province hereby advises Proponents that it does not intend to share a Proponent's Concept with the other Proponents. Proponents acknowledge that the following qualifications and provisions apply to any information in any media or format that Proponents submit or make available to the Province (including any employees, representatives or contractors thereof) in respect of or related to this STMS Project:

a) All documents, and electronic media, including the Proposals and Concepts, submitted to the Province become the property of the Province and will be held in confidence subject to the British Columbia *Freedom of Information and Protection of Privacy Act.* The Province may make such copies as the Province may require for evaluation purposes;

b) The Province will in no way be liable or responsible if another Proponent suggests a framework or idea similar to one contained in a Concept that was originally submitted by another Proponent;

c) The Province reserves the right to suggest alternative Concept structures (including alternative subcontractors of the products that are subject to standards) that may or may not be otherwise proposed by another Proponent; and

d) Proponents acknowledge that the nature of this STMS Project with multiple stakeholders and involvement by organizations within the BPS, presents a lower level of confidentiality than in previous JSP processes and as a result the Province is not responsible for any disclosure of information that a Proponent might otherwise expect to be held in confidence.

1.3.3.23 Use of JSRFP Document

No portion of this JSRFP, nor any information supplied by the Province in relation to this JSRFP, may be used or disclosed by a Proponent in any manner other than for the sole purpose of submitting a Proposal and participating in the JSP Process.

1.3.3.24 Working Language of the Province

The working language of the Province of British Columbia is English and all responses to this JSRFP must be in English.

1.3.3.25 Proposals with Joint Submissions or Subcontractors

A Proponent may submit a Proposal consisting of a joint submission by the Proponent together with one or more other entities, or which proposes the use of Subcontractors in the Final Contract. In either case, the Proponent will be the only party responsible to the Province for the Proposal, will act as the liaison and main contact with the Province in respect of the Proposal, this JSRFP and the JSP Process, and will take overall responsibility for the successful inter-relationship among the Proponent and the other entities involved in the joint submission, or contemplated as Subcontractors, as the case may be. This includes the Proponent keeping its Subcontractors fully apprised of the JSP Process and negotiations and information exchanged in respect thereof along with the Proponent making all reasonable efforts to ensure that its contractual and business relationships with its Subcontractors do not adversely affect the timing of the JSP Process or the Solution ultimately determined as part of this JSP Process. The Successful Proponent, upon becoming the Service Provider, will be responsible for the acts and omissions of its Subcontractors in providing the services. Accordingly, the Proponent who responds to this JSRFP should be the lead entity who has the capacity and will be able to demonstrate to the Province that it has the ability (financial and otherwise) to accept and fulfill this responsibility. During the JSP Process, there will be no switching of the lead entity that is the Proponent with a Subcontractor or other entity without the Province's written consent, The Province will have no obligations with respect to those other entities or Subcontractors under this JSRFP, JSP Process, the Final Contract or otherwise.

1.3.4 JSRFP Process – Joint Solution Definition Phase

Prior to participation in the Joint Solution Definition Phase, the Province will enter into a Joint Solution Definition Agreement with each of the Preferred Proponents, which will include the provisions described in Appendix C as well as such other provisions as may be determined by the Province, in its discretion, to be necessary, desirable or useful.

1.3.5 JSP Process – Due Diligence & Negotiation Phase

The Due Diligence & Negotiation Phase will substantially follow the process described in section 5.3.

1.3.6 Legal Consent

Borden Ladner Gervais LLP has provided and continues to provide legal advice to the Province in respect of the STMS Project. By submitting a Proposal each Proponent and its Subcontractors hereby expressly consent to Borden Ladner Gervais LLP continuing to act for the Province notwithstanding any unrelated solicitor-client relationship that each Proponent or its Subcontractors may have or previously had with Borden Ladner Gervais LLP.

1.3.7 Final Contract

It is anticipated that certain organizations within the BPS will enter into the Final Contract with the Province and the Service Provider. Such organizations will need access, after signing participant agreements with non-disclosure obligations, to confidential information within, and about, the Solution and the Final Contract. During the term of the Final Contract, should a new organization wish to obtain Services then they may be added as parties to the Final Contract or may acquire the Services pursuant to the mechanisms described in section 3.4.2.3.

1.3.8 Publication of Final Contract

It is the intention of the Province that most of the Final Contract will be made public. Portions of the Final Contract that will remain confidential will be identified during the Joint Solution Definition Phase and further negotiated during the Contract Negotiation Phase and will comply with the Province's Transparency Policy which is attached as Appendix E.

2 BACKGROUND

2.1 OVERVIEW

This section provides an overview of the Ministry of Labour and Citizens' Services, Workplace Technology Services, Workplace Hosting Services, and Workplace Hosting Services' responsibilities.

2.2 MINISTRY OF LABOUR AND CITIZENS' SERVICES

Two former ministries, combined under the Ministry of Labour and Citizens' Services, have in common the focus of providing excellent service: Labour provides services to employees, employers, unions, and businesses in British Columbia to build a modern work environment; and Citizens' Services plays a key role in improving how government services and information are delivered to meet the needs of citizens, business and the public sector.

The Ministry's 06/07 net budget or voted appropriation was $205.765 million. Its gross expenditures were expected to be $414.872 million. Of its gross expenditures, $209.107 million was recovered from external sources.

Many of the Ministry's business areas receive a voted appropriation of only $1,000; which requires them to operate in a disciplined, business-like manner. This '$1,000 vote structure' means that at the end of the fiscal year, expenditures must not exceed recoveries by more than $1,000.

For a government to function it needs basic tools including facilities, furniture, computers, phones, printers, email, and paper. In addition, employees must be paid; invoices and purchase orders processed; mail processed and distributed; documents printed; and office products obtained and distributed. As of April 1, 2006 accommodation and real estate services (formerly provided by BC Buildings Corporation) became a part of the Ministry. This organization ensures these services are delivered cost-effectively, efficiently and with a customer focus.

General information regarding the Ministry may be viewed at http://www.gov.bc.ca/lcs. Additional information regarding the Ministry's service plan may be viewed at the following website: http://www.bcbudget.gov.bc.ca/2007/sp/lcs/

2.3 WORKPLACE TECHNOLOGY SERVICES

Workplace Technology Services is the information technology division of the Ministry. As the steward of information technology assets and supply arrangements, Workplace Technology Services is responsible for providing cost effective management and supply of IT services to core government ministries, program managers and government employees. Workplace Technology Services is also responsible for understanding the business objectives, future directions, and unique requirements of the programs it supports.

Workplace Technology Services provides services to 19 core government ministries, several crown corporations and broader public sector organizations, and over 30,000 government employees. In support of government objectives to lower costs and improve service delivery, these clients receive reliable and cost effective services for the benefit of the citizens and businesses they serve, from Workplace Technology Services. Workplace Technology Services provides a broad range of services that include:

a) Workplace and employee productivity services such as workstations, telephones, email, electronic filing and print services, and personal digital assistants;

b) Business application enabling services such as application hosting, shared Web services, mainframe service, database support, and data storage and backup;

c) Location connectivity services such as: SPAN/BC (the provincial data network), Web domain registration, wide area (WAN) and local area connectivity, directories and authentication, and wireless network services (a WTS emerging service);

d) Business solutions such as:

   i. Common applications (used by most or all ministries; these are standard applications which must be used, if the function is required);

   ii. Shared applications (used by two or more ministries; these are optional applications which are used at the discretion of the ministry);

   iii. Software licence management; and

   iv. Consulting and professional services specializing in IM/IT solutions integration and project management.

In terms of scale and scope, the services outlined above support:

   i. More than 1,000 core-government locations;

   ii. 30,000 government employees providing service to citizens and business, as well as internal government operations;

   iii. 2000 BC schools and 600,000 students who are connected via the provincial learning network, a component of the province wide network SPAN/BC;

   iv. E-mail services for approximately 40,000 accounts; and

   v. 50,000 telephone connections, providing clear and consistent voice communications.

Workplace Technology Services currently operates within a mixed model with services being delivered by both internal resources and private sector service providers.

Workplace Technology Services provides value through aggregating demand for similar services across government, and integrating various information technology components and provider services into general service packages and customized solutions. Typically, services to broader public-sector organizations leverage those services provided to ministries and, in return, increase economies of scale to the benefit of all parties.

2.3.1 Workplace Hosting Services

2.3.1.1 Background

Workplace Hosting Services is a branch within the WTS and provides computing server platforms for processing, hosting, and storage of applications, data and information, working to agreed-upon service levels so that clients can build and run their business applications in a secure and managed environment. Consulting services are also provided as a shared or customized service offering.

Currently the Province has developed or purchased hundreds of business applications which are hosted on approximately 1,600 server platforms and one mainframe computer.

The scope of operations includes Ministry and non-ministry application needs as well as other shared service(s) or cross-government application needs such as corporate accounting services, collaboration software/middleware, shared file and print services, email, authentication services and WTS' information technology infrastructure. Current Hosting Services are provided on four main computing platforms/environments: Mainframe, UNIX, Windows and Linux that are contained primarily in the main data centre at S15 in Victoria. Several smaller data centres in Victoria and Vancouver are also under Workplace Hosting Services management.

The following figure shows the current state operational environment of Workplace Hosting Services:

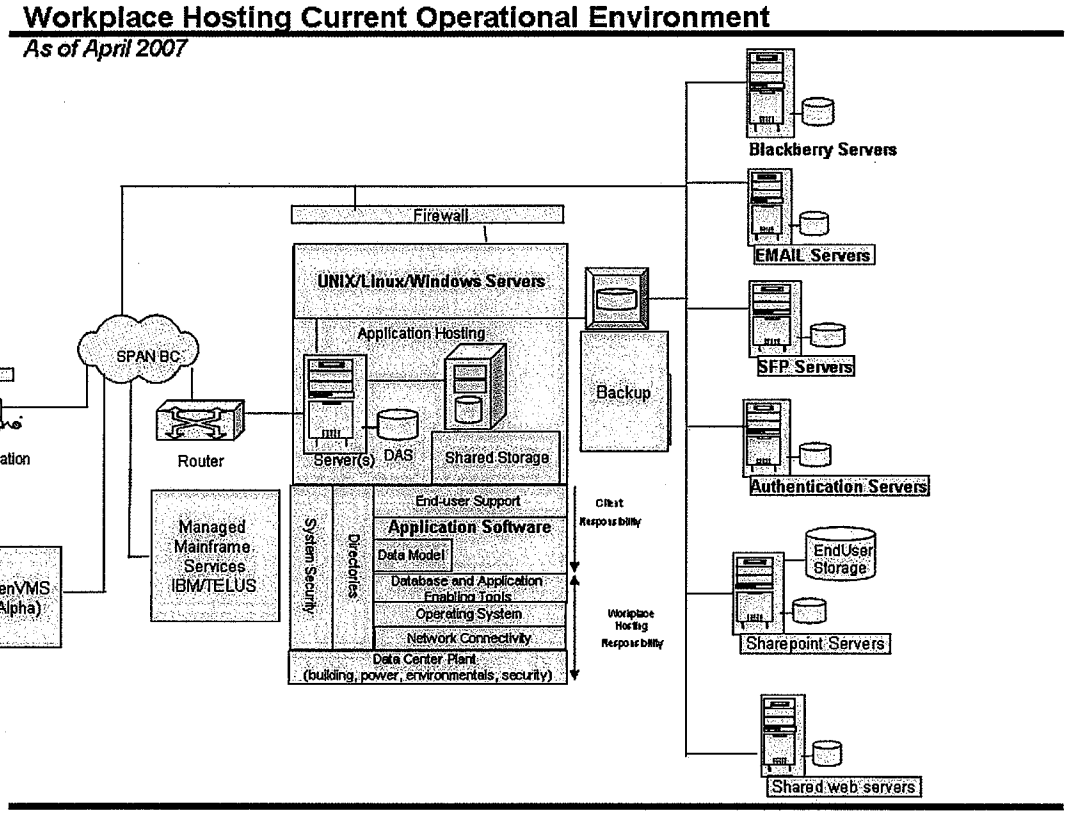


Figure 2 – Operational Environment

2.3.1.2 Long Term Business Objectives

The long term business objectives of Workplace Hosting Services are outlined as follows:

a) Maintain or enhance the stability of the information technology infrastructure;

b) Optimize the computing platform infrastructure;

c) Reduce costs to develop and deliver services and continuously explore opportunities for improved IT service delivery (including entering into business relationships with other public and private sector entities);

d) Formalize client service level agreements;

e) Develop a comprehensive human resources strategy that reflects and supports WTS' evolving business model; and

f) Actively support the objectives of WTS' overall strategy and service plan.

2.3.1.3 Current Hosting Services

The main services provided by Workplace Hosting Services include:

a) Database support - comprehensive support for database systems running on shared processors or on client-dedicated computing systems. Clients can choose from database system planning, implementation and management, as well as database and application consulting in order to tailor the service to their specific requirements;

b) Shared database service - provides a secure, reliable database environment for databases. By sharing the costs of this environment, clients benefit from a stable and managed platform at a lower cost than with a dedicated server and support staff. Included in the service is the building of the database, backups, exports, monitoring, recoveries and licensing;

c) Storage and backup

   i. Storage service - provides infrastructure and management and support activities for the storage of client's electronic data. The service is classified into multiple storage tiers, based on the performance and availability requirements of the client,

   ii. Data backup service - protects a client's data by ensuring it is backed-up (copied), stored and available electronically for use if the originals cannot be accessed. When required, the backup copies are accessible and may be restored. The Data backup service may be set up to run on an automated schedule, or provide live (online) backup for Oracle, SQL and Informix databases;

d) Application hosting service for UNIX, Linux and Windows - provides server support, management, and backup support for UNIX, Linux and Windows servers. Workplace Hosting also procures hardware, system software and application infrastructure on behalf of clients;

e) Shared web hosting service - provides a secure and reliable infrastructure for clients to develop, test and publish content for Internet, Intranet or Extranet sites. Space is provided on shared, managed web server infrastructure;

f) Mainframe service - a shared, secure MVS processing system consisting of current technology hardware components and software products. The MVS service provides a wide range of online and batch services supporting critical line-of-business client applications and includes the underlying data centre facilities services. This service is currently contracted to IBM Canada Limited (with TELUS Communications Inc. as its subcontractor);

g) OpenVMS - provides the platform or 'working environment' required for shared use by clients to develop, manage, and run their own applications. The service provides the shared environment as well as system management and technical support activities;

h) Hosting consulting and professional services - comprehensive consulting and professional services using the expertise and knowledge gained through support of hundreds of applications and information technology systems throughout the diverse WTS client base. Clients needing guidance or assistance in the management of their information technology infrastructure can draw on the tools and professional resources of WTS to investigate, analyze and resolve any performance issues which may arise; and

i) Disaster recovery planning – disaster recovery planning or business continuity planning is currently provided in a limited fashion and is entirely driven by a client's specific business needs. There is an annual disaster recovery planning exercise conducted for the mainframe only.

2.3.1.4 Current Data Centre Facilities

The Province manages four primary and a number of smaller data centres on Vancouver Island and Lower Mainland with a combined area of approximately 20,000 square feet.

Current projected growth in the Province's data centres indicates that if current growth patterns continue over a ten year period, an additional 5,000-7,000 square feet of expansion space could be required to accommodate that growth. In addition, 5,000-7,000 square feet of secondary space could be required for disaster recovery, likely in a second location outside the floodplain and potential seismic disruption.

The combined current UPS-provided power consumption is approximately 800 kW.

2.3.2 Workplace Hosting Services Challenges and Operational Risks

Workplace Hosting Services is faced with multiple challenges which adversely impact the continued provision of Current Hosting Services to its clients, and ability to transform its current service delivery model to better meet the growing and changing demands of clients. These challenges can be summarized as follows:

a) Ongoing problems with attracting and retaining skilled technical resources;

b) Insufficient resource capacity/expertise to transform the service delivery model;

c) Significant capital required to ensure server architecture is kept current;

d) Lack of flexibility in supporting temporary or peak increases in system workload, storage and back-up functions;

e) Difficulty in supporting extended-hours support and coverage;

f) Ongoing issues with keeping software and hardware at supported versions;

g) Time lags due to procurement process (four or more weeks per server); and

h) Current Data Centre Facilities are experiencing significant capacity and reliability issues.

The combination of these challenges has created an operational environment with significant risks and difficulties in improving service quality and implementing new services. To address these challenges, the Province is seeking Solutions from Proponents that will:

a) Address the operational risks of Workplace Hosting Services;

b) Transform the service delivery model to accommodate the changing needs of clients in their support of citizen-centred service delivery;

c) Determine other services that could be delivered by the Service Provider; and

d) Provide reliable (i.e. at least Tier III as per the Uptime Institute Inc. or Level 8-9 as per Brunspak) data centre facility services.

The Province may be required during the JSP Process to enter into short-term contracts in order to address the challenges and operational risks described above (in particular the capacity and reliability issues related to the Current Data Centre Facilities). It is anticipated that termination of any such contracts will coincide with the commencement of the Final Contract.

2.4 Current Service Providers

Proponents are advised that IBM Canada Limited (with TELUS Communications Inc. as its subcontractor) is currently under contract to the Ministry to deliver the mainframe services and related underlying Current Data Centre Facilities described in subsection 2.3.1.3(f) which is within the STMS Project Scope. The Province is currently negotiating a short term extension to the IBM Canada Limited contract beyond the existing expiry date of January 31, 2008.

The Pacific Technology Research Society was established by the Province in 1998 for the purpose of providing resources (through seconded employees) for some of the contracted services currently provided by IBM Canada Limited and TELUS Communications Inc. The status of the Pacific Technology Research Society is under consideration.

The Ministry also has numerous contracts with service providers to provide hardware and software maintenance services related to Current Hosting Services. The current service providers, including IBM Canada Limited, TELUS Communications Inc., Hewlett-Packard (Canada) Co., Sun Microsystems of Canada Inc., etc., are not precluded by these contracts from submitting proposals in response to this JSRFP.

For non-mainframe hosting services, the Province provides its own services in relation to the Current Data Centre Facilities.

2.5 Broader Public Sector

The Province has been engaged in discussions with organizations within the BPS regarding the STMS Project. It is anticipated that many organizations within the BPS will participate in the JSP Process either as subject matter experts, as part of the evaluation committee, or by providing input into their possible requirements for services. For example, the Provincial Health Services Authority, the Vancouver Coastal Health Authority and ICBC have agreed to participate in the JSP Process, and these organizations have indicated that they will require data centre facilities; other organizations within the BPS may also require data centre facilities. A general outline of the requirements for ICBC are included as an example in Appendix H, and it is anticipated, as other requirements from the BPS become available, they will be provided to Proponents as well. However, the timing and amount of each organization's purchase of any Services may vary.

It is the Province's intention to allow such interested organizations within the BPS to provide input into the negotiation of the Final Contract with the Successful Proponent and to purchase some or all of the Services as signatories to the Final Contract. Accordingly, Proponents should be aware that confidential information regarding the Solution, the Services and the terms of the Final Contract will need to be shared with such organizations within the BPS. If new organizations within the BPS then wish to acquire Services during the term of the Final

Contract, they will be added as parties to the Final Contract or may acquire the Services pursuant to the mechanisms described in section 3.4.2.3.

This Space Intentionally Left Blank

3 DEFINING THE OPPORTUNITY

3.1 PROJECT VISION

The Ministry is interested in receiving Proposals from qualified and experienced Proponents who are capable of delivering the Scope of the Opportunity, including hosting services and the underlying data centre facility services , and possessing the strategic business transformation experience necessary to transform Workplace Hosting Services into a world class service delivery organisation.

3.2 STMS PROJECT OVERVIEW

The STMS Project is intended to initiate a series of service delivery transitions requiring a varied degree of strategic business transformation expertise in order to address the business challenges and risks currently experienced by Workplace Hosting Services.

The initial service delivery transition to the Service Provider will include the mainframe service currently contracted to IBM Canada Limited (see section 2.4). The Province is interested in exploring, during the JSD Phase, other functions and services which could be transitioned to the Service Provider as well as new services that address the business challenges and risks. As part of this initial service delivery transition, the Service Provider will also be expected to provision the necessary data centre facility infrastructure.

The Service Provider will be required to work with Workplace Hosting Services in reviewing the business challenges and operational risks and the future direction of Workplace Hosting Services to identity additional transformational and service delivery opportunities.

Furthermore, the Ministry will also seek to jointly develop Solutions that provide the service delivery scalability and flexibility to take advantage of opportunities for the BPS to acquire Services.

All these opportunities will be more fully explored by the Ministry and Preferred Proponents during the Joint Solution Definition Phase of the JSP Process.

3.3 STMS PROJECT OBJECTIVES

3.3.1 STMS Project Business Objectives

The Province expects Proponents to jointly develop, with the Province, a Solution which will achieve the following business objectives:

a) Provide attractive and creative (financially and operationally) options for mainframe services;

b) Identify strategic transformation opportunities for Workplace Hosting Services that could address the business challenges and operational risks noted earlier (see section 2.3.2), align with the long term business objectives (see section 2.3.1.2), and transform the current service delivery structure to meet the future needs of government;

c) Identify possible Services, with an attractive business case, to be delivered by the Service Provider; and

d) Provide attractive and creative (financially and operationally) data centre facility services.

3.3.2 STMS Project Technical Objectives

The Solution is expected to achieve the following technical objectives:

a) Infrastructure technology operated 24 x 7, 365 days a year, while meeting or exceeding service levels;

b) Compliant with the Province's applicable security and privacy legislation, policies and standards in order to ensure the safeguarding of personal and other confidential information;

c) In alignment with ISO 17799, a standards framework for security;

d) Capable of scaling to accommodate the transaction load of a growing client base;

e) Allow the evolution of additional functionality in support of future initiatives; and

f) Capable of scaling to accommodate business and technology functions over time.

3.4 SCOPE OF THE OPPORTUNITY

The Scope of the Opportunity includes the STMS Project Scope and the Potential In-Scope.

The following diagram illustrates the Scope of the Opportunity:

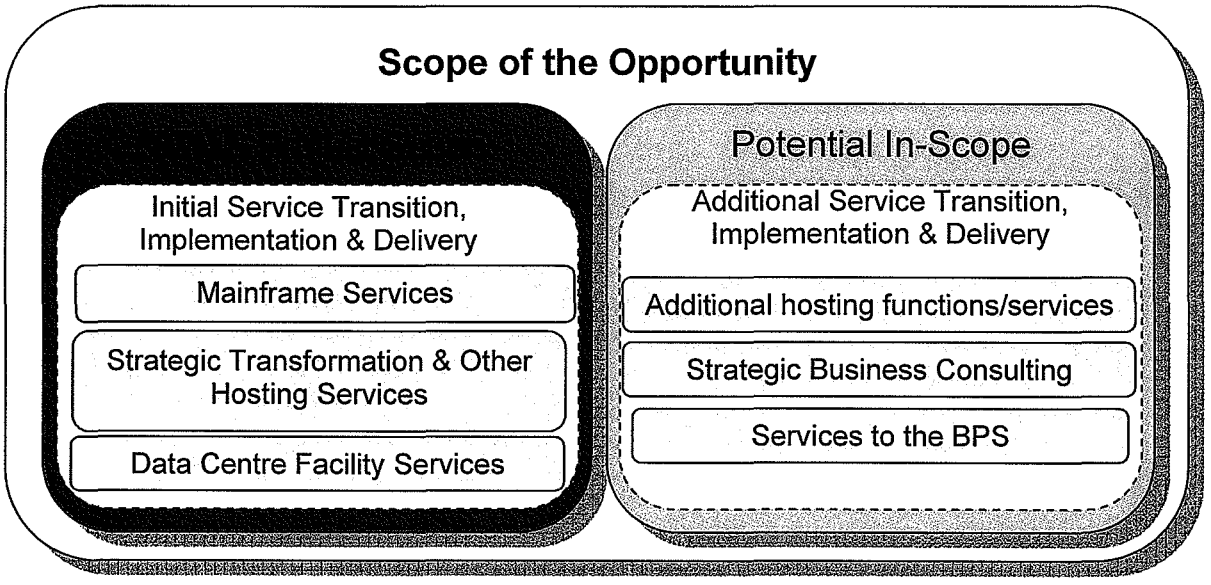


Figure 3 – Scope of the Opportunity

The term of the Final Contract will be up to fifteen years for the data centre facility services with an anticipated option to extend for an additional five years. It is anticipated that the term for the hosting services component will likely be shorter (e.g. five to seven years) with options to extend the hosting services for additional terms of up to five years but, in no event, longer than the term of the data centre facility services term.

3.4.1 STMS Project Scope

The requirements for the STMS Project that are in scope are as follows:

3.4.1.1 Mainframe Services

Workplace Technology Services provides a shared, secure MVS processing system consisting of current technology hardware components and software products. The MVS service provides a wide range of online and batch services supporting critical line-of-business Client applications.

The current processor is a 597 MIP IBM z890, running CICS, IMS, DB2, TSO and batch via 5 logical partitions (LPARS), all under the z/OS operating system (formerly known as MVS). Current disk capacity is roughly 2,910 GB, and the complex makes use of VTS tape handling a maximum of 13,300 GB.

The following figure shows the current mainframe environment:

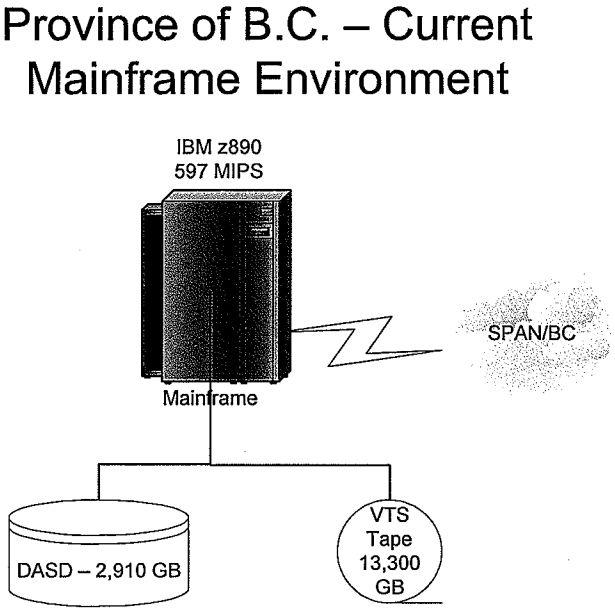


Figure 4 – Mainframe Environment

The Services will include provision and management of the z/OS mainframe platform (inclusive of the DASD, operating system and any unique software required in the WTS environment), to agreed upon service levels, and an annual disaster recovery exercise. The Province expects that the infrastructure (e.g. data centre facility), tools and processes required are included as part of the Services.

See Appendix G for more information regarding the current mainframe environment.

3.4.1.2 Strategic Transformation and Other Hosting Services

It is expected that via the JSP Process, Proponents will identify and demonstrate opportunities for service delivery model transformation that will address the project objectives (see section 3.3). Depending on the transformation strategy that forms part of

the Solution, the Province will determine which transformation services may form a part of the Services in the Final Contract.

Based on the transformation opportunities identified in the Solution, the Province will determine which hosting services will be provided by the Service Provider and which will continue to be provided by the Province. The Province expects that the infrastructure (e.g. data centre facility), tools and processes required by the Service Provider to deliver the hosting services are included as part of the Services.

3.4.1.3 Data Centre Facility Services

The Province does not believe that investing in data centre facilities is core to its business strategy, and is seeking the provision of a "managed service" for data centre facilities.

3.4.2 Potential In-Scope

The Province reserves the right during any phase of the JSP Process or during the term of the Final Contract to expand the scope of Services to be provided by the Service Provider under the Final Contract as follows:

3.4.2.1 Additional Hosting Functions/Services

In order to achieve the long-term business objectives (see section 2.3.1.2), STMS Project vision (see section 3.1) and STMS Project objectives (see section 3.3) additional functions/services may be considered for provision by the Service Provider. For example, such functions/services could include:

1. Server deployment;
2. Server management;
3. Operational system planning and support;
4. Release management;
5. Incident management;
6. Operational procurement; and
7. Disaster recovery and business continuity.

The Province expects that the infrastructure (e.g. data centre facility), tools and processes required are included as part of the Services.

3.4.2.2 Strategic Business Consulting

The Province could, at its discretion, engage the Service Provider to provide consulting services to assist with the strategic business transformation of its service delivery model

3.4.2.3 Services to the Broader Public Sector

The Province intends to enable and facilitate organizations within the Broader Public Sector in obtaining some or all of the Services, in particular data centre facility services, as follows:

a) such Broader Public Sector organizations will be signatories to the Final Contract;

b) such Broader Public Sector organizations may receive some or all of the Services as a client of the Province under the Final Contract; or

c) during the term of the Final Contract, the Province and the Service Provider may agree to other contractual mechanisms to permit such Broader Public Sector organizations to obtain some or all of the Services.

3.4.3 Out of Scope

The following are out of scope for the STMS Project:

1. Provincial network (SPAN BC);
2. Corporate policy; and
3. Corporate strategic planning.

This Space Intentionally Left Blank

3.5 PROPOSED DELIVERY APPROACH

It is envisioned that the Solution could be implemented in sequential phases, likely starting with implementation of the mainframe services component of the Solution.

Proponents should note that depending on solution development activities related to Potential In-Scope requirements and the transformational opportunities presented, other services may be scheduled for parallel implementation. For this reason, the Province expects that the Preferred Proponents will have strong transformational teams prepared to develop their Solutions with the Province during the Joint Solution Definition Phase.

As the STMS Project completes transition of the mainframe services described in subsection 2.3.1.3(f), other opportunities will be explored with the Service Provider with a view to addressing the challenges, risks and business objectives described in this document. This could include a continuation of Current Hosting Services (self provision) in combination with Services provided by the Service Provider in order to address evolving Workplace Hosting Services business needs.

3.6 INTELLECTUAL PROPERTY PRINCIPLES

3.6.1 General

The following are some general principles relating to Intellectual Property for the STMS Project:

1. Intellectual Property rights in relation to the Solution will be more fully developed in the Joint Solution Definition Phase;
2. The ownership of the Intellectual Property may depend on the economic model proposed by the Proponents;
3. Whether the Proponents intend to productize or commercialize all or part of the Solution may affect the economic model put forward by Proponents; and
4. Intellectual Property used or developed in relation to the Services may be required to be owned by or licensed to the Province.

This Space Intentionally Left Blank

3.7 PROJECT GOVERNANCE

A core team of experts are dedicated to this STMS Project, supported by the executive project sponsor who is the Deputy Minister of Labour and Citizens' Services, Lori Wanamaker.

In addition the STMS Project is overseen by a steering committee of senior executives.

Several stakeholder consultation groups will be involved during the JSP Process and will be available for ongoing consultation as subject matter experts throughout the JSP Process.

3.8 DEAL STRUCTURE AND ECONOMIC MODEL

It is the intention of the Province to enter into a single Final Contract with the Successful Proponent.

It is anticipated that the Service Provider will invest in the development of the Solution and will deliver and operate it for the term of the Final Contract. Upon the expiration of the term, the Province may enter into another competition which may result in the transfer of the continuing provision of hosting services to another service provider.

There are a variety of possible economic models that can arise from the JSP Process. Proponents are asked in section 5.7.2 to describe past large scale information technology and services delivery projects (particularly those with transformational aspects) and demonstrate to the Province their in-depth knowledge and experience in conceptualizing, designing, developing and operating financial models that are true to the spirit of the type of deal structures contemplated for the opportunity.

The Final Contract may include design, implementation and operation, all under a single economic model. The Ministry is encouraging Proponents to come forward with innovative and creative deal structures and economic models that are not based on a traditional 'time and materials' basis. Additionally, the Ministry is expecting to see the detailed information which supports the creative deal structures and economic models as part of the Joint Solution Definition Phase and final Solution presentations. Two key components of the Preferred Proponent presentations on deal structures and economic model will be the principles that the Preferred Proponents would use to integrate the Potential In-Scope opportunities within the economic model over the term of the Final Contract and that each Solution will include transfer of the majority of the risk for Service delivery from the Province to the Service Provider.

3.9 PRIVACY AND COMPLIANCE

3.9.1 Privacy

The STMS Project may entail management of sensitive health, financial and other personal information from its collection through to its destruction. The Proponent must be able to ensure that the personal information it may deal with as the Service Provider will not be disclosed and will be kept secure.

The Service Provider will be required to comply with British Columbia laws governing the collection, use and disclosure of personal information, including the *Freedom of Information and Protection of Privacy Act* (FOIPPA), the *Personal Information Protection Act*, the *Document*

Disposal Act, and any other applicable legislation. The Service Provider will be required to, at a minimum, adhere to the Privacy Protection Schedule attached as Appendix D.

Where FOIPPA is concerned, Proponents are expected to demonstrate understanding of the application of Part 2, including compliance with amendments that limit the disclosure, storage of or access to personal information outside of Canada. Proponents should keep in mind that changes to provincial legislation and policies may occur from time to time.

Proponents should note that a Solution including remote access from outside Canada to any personal information will not be acceptable to the Province. Furthermore, if any employees of non-Canadian companies need to have access to systems containing personal information within Canada, that access has to be supervised by staff from a Canadian organization.

More information on FOIPPA and related policies and guidelines of the Province is available at http://www.mser.gov.bc.ca/privacyaccess/.

Issues related to privacy, such as the role of the Information and Privacy Commissioner, and the privacy policies that apply to projects of provincial scope, will be further discussed during the Workshops and during Solution compliance activity of the Joint Solution Definition Phase.

3.9.2 Labour Relations

WTS' employees predominantly have union membership in the British Columbia Government and Service Employees' Union in accordance with the *Public Service Act*.

Activities related to labour relations will be dealt with in later phases of the JSP process.

3.9.3 Other Policies and Regulations that may impact the Solution

Proponents should be aware of, and the Service Provider will need to comply with, the Core Policy and Procedures Manual and other central policies of the Province (e.g. policies of the Chief Information Officer, more information is available at www.cio.gov.bc.ca). As part of the Joint Solution Definition Phase it is possible that specific legislation, policies and regulations that may impact a proposed Solution will be identified.

The process of disposition of assets, both current and future assets, will be further explored in a later phase of the JSP process.

Proponents should note that it is the intention of the Province that most of the Final Contract will be made public. Portions of the Final Contract that will remain confidential will be identified during the Joint Solution Definition Phase and further negotiated during the Contract Negotiation Phase but will comply with the Province's Transparency Policy, a copy of which is attached as Appendix E.

Finally, the Province is in the process of considering policies promoting environmental sustainability.

4 OVERVIEW OF THE END-TO-END JSP PROCESS

4.1 DEFINITION

A JSP Process is a multi-stage procurement process. The first phase of the JSP Process is the Proponent Qualification Phase which is designed to short-list Proponents based primarily on their capacity, capability, commitment and initial conceptual approach as described in sections 5.6.1.1 to 5.6.1.4. There follows three distinct phases consisting of a Joint Solution Definition Phase (where Solution development will occur), followed by a Due Diligence & Negotiations Phase, and ending with a Contract Negotiations Phase (where the Final Contract terms are framed, finalized and executed by the parties).

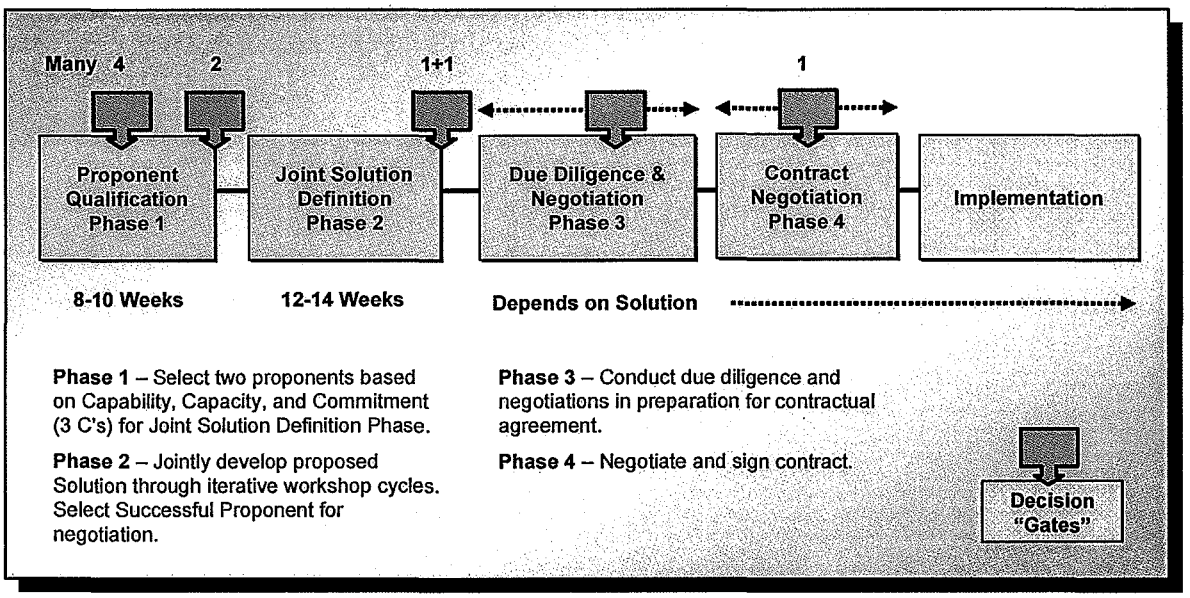


Figure 5 – JSP Process Overview

4.1.1 JSP Process Schedule

Phase	Task Activity	Anticipated Date
1. Proponent Qualification Phase	JSRFP Closing date	Jul 26, 2007
	Proponents short-listed (Stage 1)	Aug 7, 2007
	Workshops and Concept Presentations (Stage 2 and 3)	Aug 15-30, 2007
	Preferred Proponents notified	Sep 14, 2007

Phase	Task Activity	Anticipated Date
2. Joint Solution Definition Phase	Joint Solution Definition Phase kick-off	Sep 26, 2007
	Solution presentations completed	Dec 2007
	Letter of Intent signed and Successful Proponent announced	Dec 2007
3. Due Diligence & Negotiation Phase	Due Diligence & Negotiations initiated	Dec 2007
4. Contract Negotiation Phase	Contract Negotiations initiated	TBD
	Sign Final Contract	TBD

The Ministry is interested in expediting the selection process where possible, and reserves the right to adjust the preceding schedule wherever practical.

4.2 KEY SUCCESS FACTORS

4.2.1 Sharing of Risks and Rewards

Risk and reward will be explored during the Joint Solution Definition Phase and it is anticipated that the Service Provider will assume a significant portion of the risk (including, but not limited to, technology, implementation and operational risks).

4.2.2 Communications Protocol

Maintaining proper communications protocol throughout the JSP Process is important in order to protect the integrity of the JSP Process and the STMS Project, as well as to protect the interests of the Proponents and Ministry. The following communication protocol will apply during the JSP Process. The failure of a Proponent to adhere to the communication protocol may result in the Proponent being disqualified from the JSP Process.

4.2.2.1 During the JSRFP

All communication related to the JSRFP should be referred to the Government Contact listed on the front page of this JSRFP document.

4.2.2.2 Proponent Qualification Phase – Stage 2

Restricted Documents Room

Communications regarding the Restricted Documents Room must be referred to the Government Contact listed on the front page of this JSRFP document. Guidelines for use of the Restricted Documents Room will be provided to short-listed Proponents prior to the opening of the Restricted Documents Room.

For further information on the Restricted Documents Room, see section 5.1.5.

Workshops

Face-to-face communications between Proponents and Ministry representatives as part of the Workshops is expected (see section 5.1.6). Please note that the Ministry reserves the right to withhold information at the Workshops that may impact its negotiating position during the subsequent phases of the JSP Process.

This Space Intentionally Left Blank

5 THE JSP PROCESS AND EVALUATION CRITERIA

5.1 PROPONENT QUALIFICATION PHASE

5.1.1 Approach and Overview

A Proponent's Proposal in response to this JSRFP is the initial step in qualifying to participate in the JSP Process. Proponents will be short-listed based on overall capability, capacity, commitment and initial conceptual approach. Preferred Proponents will then be selected based on their proposed Concept. Proponents should keep in mind that the Ministry is not only looking for information on how to provide these Services and achieve the key objectives, but also on proof that the Proponent has successfully designed, implemented and operated similar services.

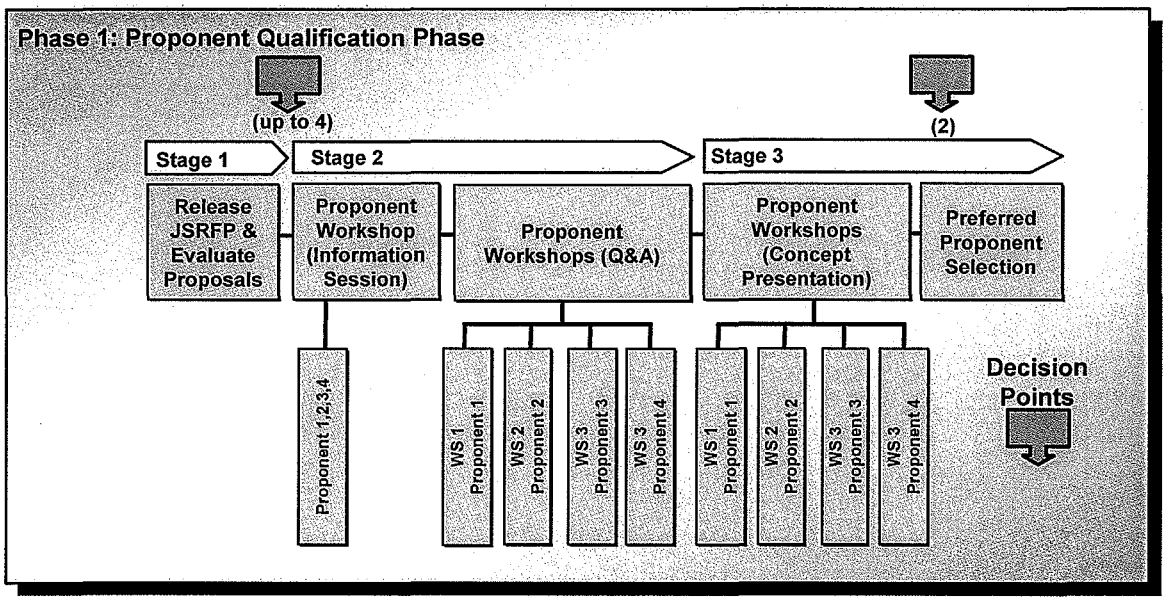


Figure 6 – Proponent Qualification Phase

Identification of the Preferred Proponents is based on the assessment of a Proponent's capacity, capability and commitment to work with the Ministry in developing a Solution that meets the goals of the Ministry and desired business outcomes for the STMS Project. The Proponent will move through the Proponent Qualification Phase, from Stage 1 (evaluation of Proposals), gain more knowledge of the Ministry business environment and needs during Stage 2 (Workshops) and finally deliver a more focused but still conceptual solution during Stage 3 (evaluation of Concepts). The Concepts provided by the Preferred Proponents will be reviewed in the Joint Solution Definition Phase. The Proponents should understand that the Concepts may be subject to significant change as the Joint Solution Definition Phase progresses.

5.1.2 Role of Lead Proponent in the JSP Process

Proponents should take care when determining their initial team structure and identifying the lead entity to be the Proponent. The Province's intention is not to permit the firm who is identified as the lead entity that is the Proponent to swap its primary role with a Subcontractor

later in the process. Please note that this does not preclude a new entity from being created by the Successful Proponent to enter into the Final Contract resulting from this JSP Process.

5.1.3 Release JSRFP & Evaluate Proposals

The Proponent Qualification Phase commences on the release of the JSRFP.

Upon completion of the evaluation of the Proposals, a short-list of up to four Proponents will be created and those Proponents will be invited to participate in Stage 2 of the Proponent Qualification Phase. The remaining Proponents will be advised of their standing in writing and offered debriefing sessions. The Ministry intends to hold the debriefing sessions after the execution of the Final Contract but may at its discretion hold these sessions sooner.

5.1.4 If Only Two Proponents

If as a result of the evaluation of the Proposals in Stage 1, the Ministry determines that only two Proponents are deemed to be qualified, then the Ministry reserves the right to consider these short-listed Proponents as Preferred Proponents and to proceed directly to the Joint Solution Definition Phase. In this case some aspects of the Workshops may be performed during the early part of the Joint Solution Definition Phase in order to set the stage for Solution development. The Ministry also reserves the right to invite the two Preferred Proponents to present either their Concepts or their capacity, capability and commitment to the Ministry to ensure that they have the necessary capacity, capability and commitment required to undertake the STMS Project and deliver the final Solution. These presentations may take place either prior to the commencement of the Solution definition activities, or at any other time during the Joint Solution Definition Phase.

5.1.5 Restricted Documents Room

Immediately prior to the Workshops, short-listed Proponents will be provided with access to the Restricted Documents Room, if one is established. The Restricted Documents Room will serve as a repository for information relevant to the preparation of the short-listed Proponent's Concept presentations. The room may be a physical location in Victoria, British Columbia or created virtually. Access will be controlled and monitored to ensure equitable viewing time for each of the short-listed Proponents. Inquiries regarding the Restricted Documents Room must be referred to the government contact listed on the front of this JSRFP document.

5.1.6 Stage 2 – Workshops

The purpose of the Workshops is to allow short-listed Proponents the ability to further explore the Scope of the Opportunity and to provide an avenue for them to assess whether the STMS Project is of sufficient interest to engage in a significant amount of work at the Joint Solution Definition Phase and, if the Proponent is the Successful Proponent, at the Due Diligence & Negotiation Phase and the Contract Negotiation Phase. These Workshops, which will be held in Victoria, British Columbia, are not evaluated.

The guidelines that will govern the Workshops are outlined below. The Ministry reserves the right to alter these guidelines (and any scheduling) as needed, but will only do so after notifying the short-listed Proponents.

a) The Ministry will deliver a half-day information session to all short-listed Proponents. This information session will be unidirectional and with all short-listed Proponents present at the same time, to ensure that all short-listed Proponents are given the same information.

b) A second half-day session will be reserved for each short-listed Proponent's staff to question the Ministry team so as to further explore the material presented or to ask questions that the short-listed Proponent feels are needed in order for it to deliver a Concept at Stage 3 of the selection process. Please note that there will be no allowance for a follow-up Workshop. Wide latitude will be afforded to the question period and short-listed Proponents may manage the meeting in the manner that they deem most useful (e.g. break out sessions where appropriate).

c) While the Ministry will make every effort to ensure that pertinent people are available to answer queries, there may be some questions that cannot be answered during the second session. In this case every effort will be made to communicate the response to the short-listed Proponent within one working day of the Workshop. The Ministry will, however, not be liable for any delays whatsoever in providing a response to any unanswered questions within that period.

d) The Workshops will not be recorded and all questions asked by a short-listed Proponent will be considered proprietary and not released to other short-listed Proponents. In addition, answers to questions asked during the Workshops which could not be answered by Ministry staff will be communicated in writing to the respective short-listed Proponent only. All questions asked prior to or after the Workshops should be submitted in writing to the contact person indicated on the front of this JSRFP. Responses to these questions may be communicated to all short-listed Proponents. The Ministry reserves the right, however, to disseminate information related to the Province or the STMS Project arising as a result of questioning in any one of the Workshops, to all short-listed Proponents if, in the opinion of the Ministry, the information is related to a matter that all Proponents will need to know in order to prepare for the presentations.

e) The Ministry will not require short-listed Proponents to bring specific staff to the Workshops. Each short-listed Proponent should decide who from their organization is best suited to gather the necessary information.

5.1.7 Stage 3 - Proponent Concept Presentations

On completion of the Workshops, short-listed Proponents will be given time to assess the information they have gathered during their Workshops and formulate a Concept for presentation to the evaluation committee in Stage 3. Section 5.6.1.4 describes the evaluation criteria that will be used at Stage 3. Prior to the presentations, the Province will provide more information regarding the presentation format and evaluation criteria.

A transcription or minutes may be taken of the Stage 3 presentations.

Presentations will be time limited. The time allocated will include time for the evaluation committee to ask questions.

The identification of the Preferred Proponents will be determined by evaluation of the Concept presentation. Each short-listed Proponent is required to supplement its presentation with speaking notes and a paper and electronic copy of its Concept presentation.

5.1.8 Preferred Proponents Selection

On completion of the evaluation process, the Ministry will tabulate the evaluation results from Stage 3 of the Proponent Qualification Phase and rank the short-listed Proponents. The top two ranked short-listed Proponents will be deemed Preferred Proponents and will be invited to engage in the Joint Solution Definition Phase.

5.1.9 Post Presentations and Debriefings

Once the top two Preferred Proponents have been declared, a Joint Solution Definition Agreement will have to be executed by the Ministry and each of the two Preferred Proponents prior to commencing the Joint Solution Definition Phase activities.

In the event that Joint Solution Definition Phase activities or negotiations with one of the Preferred Proponents fail, the Ministry reserves the right to contact the next highest ranked short-listed Proponent and invite them to engage in Joint Solution Definition Phase activities with the Ministry.

Proponents who are not invited to the Joint Solution Definition Phase may request a debriefing session which will be scheduled by the Province after the execution of the Final Contract.

5.2 JOINT SOLUTION DEFINITION PHASE

The Joint Solution Definition Phase of the JSP Process will require significant investment on the part of the Ministry as well as the Preferred Proponents. The Joint Solution Definition Agreement that is signed by the Province with each of the Preferred Proponents will govern the conduct of the remaining phases of the JSP Process.

Preferred Proponents are cautioned not to delay in negotiating the Joint Solution Definition Agreement as once one Preferred Proponent has satisfactorily executed the Joint Solution Definition Agreement the discovery cycle of the Joint Solution Definition Phase described in section 5.2.2 may begin immediately with that Preferred Proponent. The Joint Solution Definition Phase will be held in Victoria, British Columbia. The following figure should be used as a guideline and timelines may be modified as required by the Province.

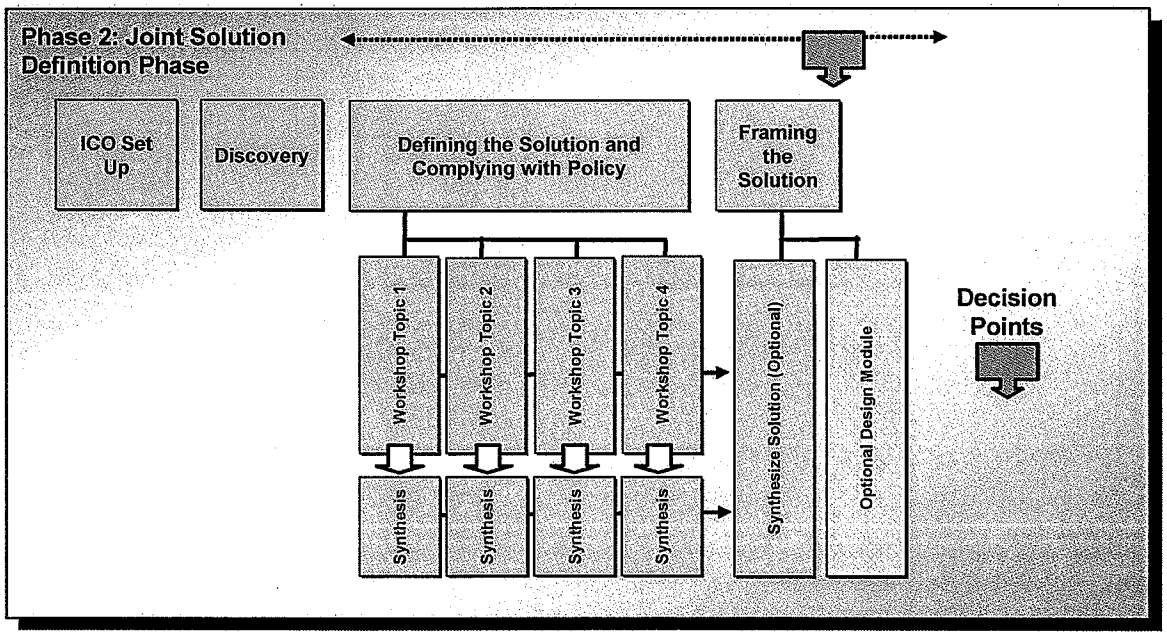


Figure 7 – Joint Solution Definition Phase

The core objective of the Joint Solution Definition Phase is to work with both Preferred Proponents to define Solutions including the economic models and deal structures for the STMS

Project. These activities (and series of meetings) will be performed jointly with the Ministry and Preferred Proponent teams but independently with each Preferred Proponent on their Solution. The Successful Proponent and their Solution will be subject to due diligence and negotiations during the subsequent Due Diligence & Negotiation Phase of the JSP Process.

5.2.1 Information Control Office

The Ministry plans to establish an Information Control Office that will serve as a central repository of information used to facilitate the exchange of confidential information between the Preferred Proponents and the Ministry. The function of this office is to ensure that confidential information provided by the Preferred Proponents is kept segregated from each other and that Joint Solution Definition Phase activities are facilitated.

Details of this office will be provided to the Preferred Proponents as the JSP Process progresses.

5.2.2 Discovery Cycle

The discovery cycle is a one time period of activity when Preferred Proponents may be permitted access to Ministry staff, documents, technology assets and records and service metrics (where applicable) as well as other information that a Preferred Proponent may consider necessary in order to prepare for creative Solution definition. Please note that this period is not guided by the Ministry.

5.2.3 Defining the Solution and Complying with Policy

This period of activity consists of a series of iterative topic specific workshops designed to define the STMS Project Scope, the potential timing to benefit realization, the nature of the deal structure, and economic model. The Preferred Proponents will be working independently from each other, with the Ministry's STMS Project team, in jointly formulating a Solution to meet the STMS Project objectives.

While the Concept provided at the Preferred Proponent's presentation during Stage 3 of the Proponent Qualification Phase will be used as a basis for the Solution, it is possible that information gathered during the discovery cycle or as a result of discussions with the Ministry during this cycle may result in an entirely different approach being considered. It is likely that the Solutions developed by the Preferred Proponents may be very different.

Each topic is envisioned to be explored over a series of two half-day workshops with each Preferred Proponent. These workshops are typically spread over one week (e.g., 2 days of workshops per week with one Preferred Proponent in the morning and the other Preferred Proponent in the afternoon). For each topic, the results of the half-day workshops are brought together, typically in the subsequent week, at the synthesis workshop. The Ministry expects that the Solutions will be very creative. The actual schedule will be communicated to the Preferred Proponents as part of the information session launching the Joint Solution Definition Phase.

The Ministry will ensure that its decision makers are at the table so that decisions are expedited and the Joint Solution Definition Phase of the JSP Process successfully concluded.

As the economic model, business processes and technology aspects of the Preferred Proponent's Solution are being formulated, the Preferred Proponents and the Ministry will need to continually assess the evolving Solution framework for compliance with the legislation and policies of the Province. This process will include a series of iterative cycles where the Solution

parameters are measured against functions such as: conformance with privacy laws, other statutes and policies, and existing agreements that may impact the Solution.

5.2.4 Framing the Solution

At this point in the Joint Solution Definition Phase, the Preferred Proponents will have formulated a Solution approach that incorporates work on a proposed deal structure, associated economic model, and Solution parameters addressing the scope of requirements and will have been tested against government policy and standards.

A period of Solution synthesis may take place on the overall model after which the Ministry will perform a final evaluation to determine the Successful Proponent. The final evaluation will likely be based on the Preferred Proponent's Solution in the areas outlined in section 5.6.1.5. The Ministry intends to release a Proponent's guide to the Preferred Proponents that outlines the evaluation criteria that will be used as a basis for determining the Successful Proponent.

Once a Successful Proponent has been announced, the remaining Preferred Proponent will be designated as the 'vendor-in-waiting'. In the event negotiations with the Successful Proponent fail, the Ministry reserves the right to contact the 'vendor-in-waiting' Preferred Proponent and invite it to enter into the Due Diligence & Negotiation Phase.

5.3 DUE DILIGENCE & NEGOTIATION PHASE

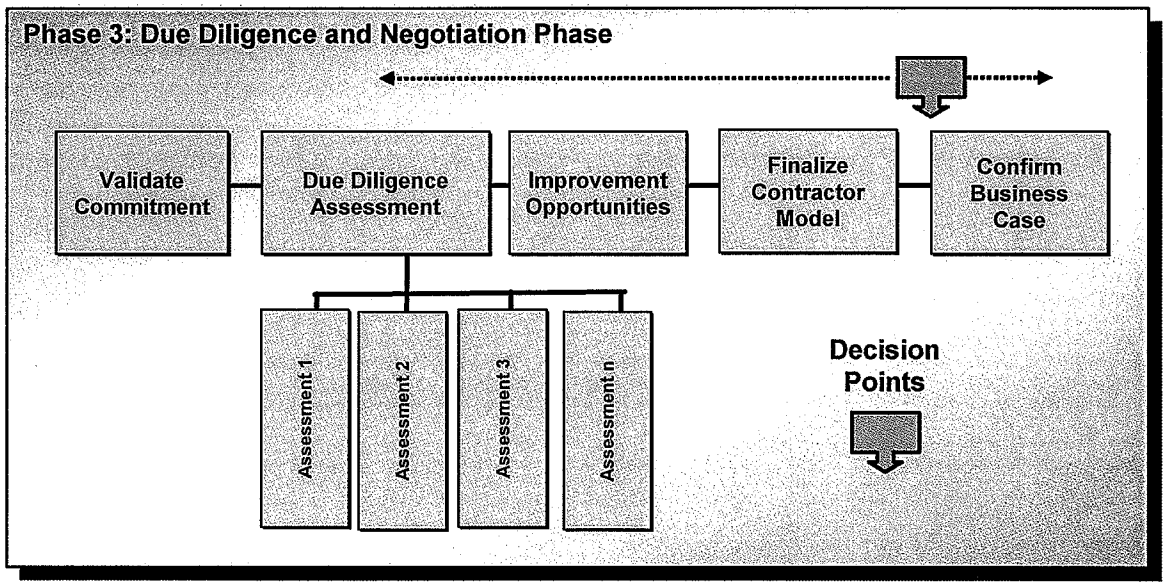


Figure 8 – Due Diligence & Negotiation Phase

Once a Successful Proponent has been chosen, the Province expects that a Letter of Intent will be signed by the parties and be followed by an announcement to the public. The Letter of Intent will be in such format and contain such detail as determined by the Province. It will include certain terms and conditions that the Province intends to include in the Final Contract. A draft copy of those terms and conditions will be provided to Preferred Proponents during the Joint Solution Definition Phase.

The Due Diligence & Negotiation Phase will begin with a period of due diligence where both the Successful Proponent and the Ministry will engage in activities to ensure that the Solution

developed during the previous Joint Solution Definition Phase is validated against detailed information.

5.3.1 Validate Commitment

An early activity in this phase is validation of the prospective business structure and of the Solution framework presented by the Successful Proponent entering into this phase. The Letter of Intent will make reference to the Successful Proponent's Solution framework as the approach of choice.

A series of activities will take place to set the stage for detailed due diligence and negotiations. This includes establishment of both the Ministry and Successful Proponent's negotiating and supporting infrastructure (tools and resources), meeting schedules, subject areas and rules of engagement as applicable.

5.3.2 Due Diligence Assessment

This period of activity is primarily for the Successful Proponent to detail its understanding of the parameters impacting successful delivery of the Solution formulated in the previous Joint Solution Definition Phase. This includes detailed verification of information used to design the Solution, assumptions reviewed and accepted or referred to negotiations. The Province may in addition, perform further due diligence on the Successful Proponent to verify its current financial and operating capacity to deliver on and commit to the statements made in the Solution framework. The Province may also decide to do further reference checks, including site visits.

5.3.3 Confirm Solution

On conclusion of the due diligence work, the Solution coming out of the previous Joint Solution Definition Phase will be refined and include discussions around governance structure, strategic and tactical plans related to the business transformation aspects of the STMS Project and guiding principles that describe how the Service Provider model will operate over the term of the Final Contract. In addition, the deal structure model will have been completed and prepared for incorporation into the Final Contract.

5.4 CONTRACT NEGOTIATION PHASE

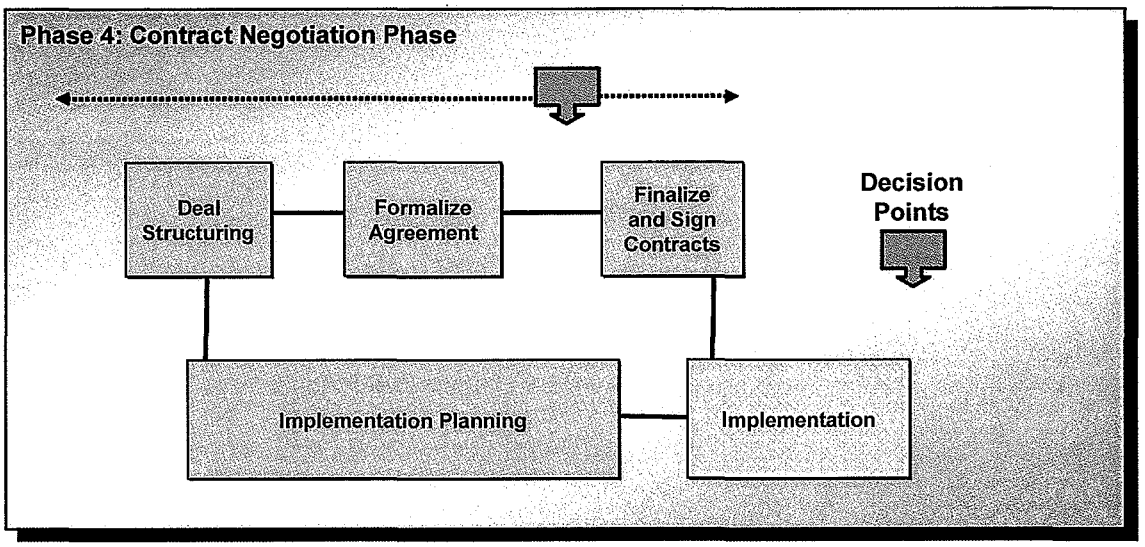


Figure 9 – Contract Negotiation Phase

The Contract Negotiation Phase marks the final phase of the JSP Process. The terms and conditions appended to the Letter of Intent signed at the commencement of the Due Diligence & Negotiation Phase will be included in the Final Contract.

Activities will include interest based negotiations, a structured negotiation process and will require negotiation commitment both from the Province and from the Successful Proponent. Concluding negotiations will in part be dependent on the Successful Proponent having those people responsible for delivery participating in negotiations, the obligation on the Successful Proponent to keep its Subcontractors involved and informed and timely escalation and resolution of issues.

Substantive activities will include final negotiation of the design and implementation parameters for the Solution and overall economic model and deal structure, governance and operational plans necessary to operate and maintain STMS and provide the associated services.

The negotiations will also include discussion on opportunities and mechanisms for mutual re-negotiation of the Final Contract, to respond to changes in the parties' respective business environment, as the relationship evolves over the term of the Final Contract. Work on the Solution (including development of STMS) will not start until the Final Contract has been executed with the Province.

There are three (3) key components that describe how the Contract Negotiation Phase – phase 4 will proceed.

5.4.1 Deal Structuring

A period of deal structuring will take place once the Solution has been finalized and agreed upon. The final term sheet will be produced, contract structure determined and final decision to proceed with the Final Contract will be made.

5.4.2 Negotiating and Drafting the Agreement

During this period of activity the Final Contract will be negotiated and drafted. Further details with respect to this phase will be provided in the Joint Solution Definition Agreement.

5.4.3 Finalize and Sign Contract

Once the Final Contract is ready for execution, both the Province and Successful Proponent will need to obtain the necessary approvals to sign the Final Contract. On signing, a public announcement may be made and implementation of the Final Contract will begin. Any public announcement by the Service Provider is to be approved by the Province before release.

5.5 DECISION POINTS

The Province reserves the right to apply a decision point at any time from the Joint Solution Definition Phase through to the end of the JSP Process and either suspend, terminate or re-start discussions or negotiations with any of the Proponents. Any determination to invoke a decision point will reside with the Province.

At various points in the JSP Process, the Province may request that the Preferred Proponents or the Successful Proponent, as the case may be, prepare and deliver a presentation to the Province so as to assess the progress of the activities to date. These presentations will be used to assess the state of the respective discussions and to determine whether the JSP Process approach continues to be appropriate.

This Space Intentionally Left Blank

5.6 Evaluation Criteria

5.6.1 Proponent Qualification Phase - Evaluation Criteria

Selection is based on evaluation by the evaluation committee of a Proponent's ability to demonstrate its capacity, capability and commitment to perform the services within the Scope of the Opportunity. Identification of the Preferred Proponents is based on performance over a two-stage evaluation process separated by a Workshop activity with each short-listed Proponent. The evaluation will proceed as follows:

5.6.1.1 Mandatory Criteria

All Proposals that have satisfied the mandatory criteria will be evaluated according to the criteria described below. Failure to satisfy any one or more of the mandatory criteria will result in disqualification from the JSP Process.

	Mandatory Criteria
1	The Proposal must be received at the closing location before the specified closing time or it will not be accepted.
2	The Proposal must be delivered by courier or hand delivered (not sent by mail, facsimile or e-mail).
3	The Proposal must be in English.

5.6.1.2 Proponent Qualification Phase - Stage 1 Evaluation Criteria

Proposals will be evaluated based on the evaluation criteria listed in the following table *Stage 1 Evaluation Criteria*.

Any Proponent who fails to meet any one of the minimum scores will be disqualified from the JSP Process without further consideration.

On completion of the Stage 1 evaluation process, the scores will be tallied and Proponents ranked. Up to the four (4) top ranked Proponents will be invited to participate in the Stage 2 Workshops. Scores achieved in Stage 1 will not be carried forward. However, information provided in the Proposals may be referenced throughout the JSP Process.

The remaining Proponents, who were not selected to proceed to Stage 2 Workshops, will be advised of their ranking and offered debriefing sessions. Sessions will likely be held after the Final Contract has been executed.

Section 5.7 provides detailed response guidelines and further information on each of the evaluation criteria outlined in the table below for Stage 1 of the Proponent Qualification Phase.

If a Proponent intends to either submit a joint Proposal with one or more Subcontractors, or intends to use the services of Subcontractors in the Final Contract, then the response to specific evaluation criteria should include information regarding the Proponent and the Subcontractor(s) (as indicated below in brackets). Where a choice is indicated (e.g. Any) the intent is to enable the Proponent to present the best credentials from within the

companies that form part of the Proposal. All other responses must be in relation to the lead entity that is the Proponent although responses about Subcontractor(s); may be added (Proponent plus); should be added (All); or are not be permitted (Proponent).

(Proponent) means a response regarding the lead entity that is the Proponent.

(Any) means a response regarding the Proponent **or** any of its Subcontractors.

(All) means a response regarding the Proponent **and** each of its Subcontractors.

(Proponent plus) means a response regarding the Proponent and, if applicable, any of its Subcontractors.

Stage 1 Evaluation Criteria	**Points Available**
Capability (see sections 5.7.2.1)	50 points (minimum score 30 points)
a) Proponent Profile (All)	
b) Demonstrated experience with transition planning and transitioning services of similar size and magnitude to the Scope of the Opportunity (Proponent plus)	
c) Demonstrated experience with delivering services similar to the Scope of the Opportunity (Proponent plus)	
d) Demonstrated experience with strategic business transformation (Proponent plus)	
e) Demonstrated experience managing employee transitions (preferably union) (Proponent plus)	
f) Demonstrated experience ensuring privacy protection and security in the management of government and other public sector information (Proponent plus)	
g) Demonstrated experience in designing and implementing complex economic models, engaging in long term commercial arrangements and experience in deal structuring (Proponent)	
h) Demonstrated experience managing complex project delivery with multiple stakeholder groups, and competing priorities (Proponent)	
i) Demonstrated experience with organizational change management for complex projects (Proponent Plus)	

Stage 1 Evaluation Criteria	Points Available
Capacity (see section 5.7.2.2) (100% of Capacity points available)	25 points (minimum score 15 points)
a) Corporate and financial capacity (Proponent)	
b) Demonstrate ability to assume and manage risk (Proponent)	
c) Demonstrate capacity to design, transition, implement, and operate services within the Scope of the Opportunity (Proponent)	
Commitment (see section 5.7.2.3) (100% of Commitment points available)	10 points (no minimum score)
a) Commitment of staff to engage in the JSP Process and STMS Project (All)	
b) Commitment to a long term relationship with the Province (Proponent)	
c) Commitment to environmentally sustainable service delivery practices (Any)	
High level concept (see section 5.7.2.4) (100% of high level concept points available)	15 points (no minimum score)
a) Provide a high level concept that addresses Workplace Hosting Services' business challenges, risks and objectives related to the Scope of the Opportunity (Proponent)	
TOTAL	**100 points**

5.6.1.3 Proponent Qualification Phase - Stage 2

All short-listed Proponents will be invited to participate in individual Stage 2 Workshops with the Ministry. Immediately prior to the Workshops, the Restricted Documents Room may open (see section 5.1.5).

The Workshops provide an opportunity for the short-listed Proponents to further explore the STMS Project to produce a Concept for delivery at the Stage 3 presentations.

Note: Stage 2 will not be scored.

5.6.1.4 Stage 3 Evaluation Criteria

On completion of Stage 2 of the Proponent Qualification Phase, short-listed Proponents will be asked to develop a Concept for presentation to the evaluation committee. Section 5.1.7 describes the format of the presentations.

The Concept accounts for 100% of the total evaluation score of Stage 2 and Stage 3.

The Province will finalize the evaluation criteria for Stage 3 prior to opening of the Proposals and will distribute the finalized evaluation criteria to the short-listed Proponents.

Stage 3 Evaluation Criteria	**Stage 3 Weighting**
Vision	**TBD**
Each Proponent should describe how their Concept aligns with and supports the Ministry's and WTS' overall role as described in this JSRFP. Each Proponent should describe how their Concept addresses each component of the Scope of the Opportunity.	
Business challenges, risks and transformation	**TBD**
Each Proponent should describe their understanding of the business challenges and risks described in section 2.3.2. Each Proponent should describe how their Concept addresses the business challenges and risks described in section 2.3.2 Each Proponent should describe how they would propose transforming the current service delivery structure.	
Client engagement approach (in transformation)	**TBD**
Each Proponent should describe how their Concept addresses the needs of clients' during transformation and service transition, and how their approach will minimize service impacts on customers.	
Services transition and operation	**TBD**
Each Proponent should describe how their Concept will address the transition and the operation of the Current Hosting Services. Each Proponent should describe their approach for transitioning services. Each Proponent should describe their proposed approach for provisioning the underlying infrastructure required for the Concept.	

Stage 3 Evaluation Criteria	Stage 3 Weighting
Labour Issues	**TBD**
Each Proponent should describe their approach for dealing with potential labour issues, and how their Concept will address these issues.	
Privacy and Security	**TBD**
Each Proponent should describe their proposed approach to providing exceptional privacy and security measures, including, at a minimum, complying with privacy laws and the contractual obligations described in Appendix D. In addition, each Proponent should describe how their approach to security will align with Province security and privacy policies (see section 3.9.3)	
Intellectual Property	**TBD**
Each Proponent should describe their approach to Intellectual Property in their Concept. Each Proponent should describe how their Concept is in alignment with the Intellectual Property principles outlined in section 3.6.	
Governance and Risk	**TBD**
Each Proponent should describe their governance approach for the STMS Project. Each Proponent should describe key issues and, to the extent that there are potential barriers, the resolution of such barriers, to complying with their approach to achieving a mutually beneficial governance model. To the extent known, each Proponent should describe the key risks associated with the STMS Project. Each Proponent should describe their high-level approach to allocate, manage and mitigate risk.	

Stage 3 Evaluation Criteria	Stage 3 Weighting
Deal Structure and Economic Model	**TBD**
Each Proponent should describe their proposed deal structure and supporting reasoning for such structure. Each Proponent should provide an overview of their proposed economic model. Each Proponent should describe their proposed pricing approach to transitioning, implementing and operating of Services in the proposed Concept. Each Proponent should describe the areas where they envision risk and reward sharing. Each Proponent should describe key issues and potential barriers to achieving their proposed economic model.	

The Concept to be delivered at the presentations should address the broad factors described above. Proponents are required to provide slides with speaker notes in paper and electronic format of the Concept presented to the evaluation committee. The Ministry acknowledges that the final Solution may be substantially different from the Concept following the Joint Solution Definition Phase.

On completion of the Stage 3 evaluation process, the scores will be tallied, and the short-listed Proponents will be ranked. The top 2 (two) short-listed Proponents will be deemed the Preferred Proponents and invited to the Joint Solution Definition Phase. (See also section 5.2).

5.6.1.5 Joint Solution Definition Phase Decision Criteria

Once the Preferred Proponents have been identified, a period of Joint Solution Definition activities will take place that culminates with the Preferred Proponents each completing a Solution and business case that describes their proposed commercial arrangement. The Ministry's executive (sponsor team) who was engaged with the Preferred Proponents during the iterative cycles of the Joint Solution Definition Phase will convene and determine which Preferred Proponent will be deemed the Successful Proponent and thereby invited to sign a Letter of Intent with the Ministry.

The Ministry will request that the Preferred Proponents present their Solution to the sponsor team where the following criteria will be assessed against the business goals and objectives of the Ministry.

(Note: The Ministry reserves the right to alter these criteria provided it does so prior to the commencement of the Joint Solutions Definition Phase, in which case, written notice of any alterations will be provided to the Preferred Proponents prior to the commencement of the Joint Solution Definition Phase).

Joint Solution Definition Phase Decision Criteria
1. Hosting Services and Data Centre Facility Services 2. Business Transformation 3. Governance / Technology Standards / Privacy / Security 4. Deal Structure 5. Economic Model

The more detailed decision criteria (e.g. labour, Intellectual Property, environmental sustainability, etc.) and governing process will be communicated to the Preferred Proponents upon the signing of the Joint Solution Definition Agreement (which must be signed prior to the commencement of the Joint Solution Definition Phase) and in a more detailed form in the proponent guidelines provided to the Preferred Proponents prior to the final presentations.

On completion of the evaluation, the Ministry will announce the Successful Proponent and the Due Diligence & Negotiation Phase will commence as described in section 5.3.

This Space Intentionally Left Blank

5.7 PROPONENT RESPONSE GUIDELINES

5.7.1 Proposal Format

Proponents are asked to assist the evaluation committee by structuring their Proposals in a consistent manner. The required Proposal format is described below:

a) JSRFP cover page;

b) Signed letter in substantially similar form to that of Appendix A;

c) Table of contents;

d) Executive summary;

e) Checklist of mandatory requirements;

f) Body of the Proposal (see section 5.7.2 below for questions that require response);

g) Corporate references; and

h) Appendices.

5.7.2 Proposal Guidelines

The Province intends to evaluate Proponents on their capability, capacity, commitment and high level concepts in relation to the Scope of the Opportunity.

If a Proponent intends to either submit a joint Proposal with one or more Subcontractors, or intends to use the services of Subcontractors in the Final Contract, then the response to specific evaluation criteria should include information regarding the Proponent and the Subcontractor(s) (as indicated below in brackets). Where a choice is indicated (e.g. Any) the intent is to enable the Proponent to present the best credentials from within the companies that form part of the Proposal. All other responses must be in relation to the lead entity that is the Proponent although responses about Subcontractor(s); may be added (Proponent plus); should be added (All); or are not be permitted (Proponent).

(Proponent)	means a response regarding the lead entity that is the Proponent.
(Any)	means a response regarding the Proponent or any of its Subcontractors.
(All)	means a response regarding the Proponent and each of its Subcontractors.
(Proponent plus)	means a response regarding the Proponent and, if applicable, any of its Subcontractors.

5.7.2.1 Capability

a) Proponent Profile (All)

Each Proponent should include a corporate profile that details background information on the Proponent, and any Subcontractors, including for each the year they were established; corporate ownership and hierarchy, jurisdiction, corporate strategic direction; area of recognized expertise in the market place; an overview of the corporate information including size, revenues, market and geographic coverage.

b) Demonstrated experience with transition planning and transitioning services of similar size and magnitude to the Scope of the Opportunity (Proponent plus)

Each Proponent should describe their experience and any Subcontractors' experience as the case may be, in transitioning and delivering solutions of similar scope and magnitude to the Scope of the Opportunity. The information provided should demonstrate how this experience relates to the STMS Project and why the experience is evidence of the Proponent's capability to design and implement required aspects of the Scope of the Opportunity. In addition, each Proponent should describe how they have transformed operations, similar in size and scope to the Scope of the Opportunity, with minimal or no impact to customers and the services being delivered by the Proponent.

Each Proponent should describe how experience gained from past projects is relevant to the business situation currently faced by Workplace Hosting Services. The preference is that the project examples be based on projects in the infrastructure hosting services environment.

Each Proponent should support their statements with examples and include information that describes the size and complexity of the engagement(s). Where possible, the Proponent should provide examples that have similarities to the Scope of the Opportunity.

c) Demonstrated experience with delivering services similar to the Scope of the Opportunity (Proponent Plus)

Each Proponent should describe its experience in delivering services similar to the Scope of the Opportunity. The information provided should demonstrate how this experience relates to the Scope of the Opportunity and why the experience is evidence of the Proponent's capability to deliver a project similar to the Scope of the Opportunity.

Each Proponent should describe how experience gained from past projects is relevant to the business situation currently faced by the Workplace Hosting Services.

Proponents should support their statements with examples and include information that confirms the size and complexity of the engagement(s). Where possible, give examples that are comparable to the Scope of the Opportunity.

d) Demonstrated experience with strategic business transformation (Proponent Plus)

Using recent examples, each Proponent should describe where they have recently worked jointly with a client organization to develop a strategy for business transformation. The example should demonstrate where the Proponent has worked with the client, over a long term, to successfully implement the strategy.

e) Demonstrated experience managing employee transitions (preferably union) (Proponent plus)

Provide examples where the Proponent, or any Subcontractor as the case may be, has experience managing an employee transition project. Describe: the high level approach taken to transition employees, challenges faced, including the number of employees transitioned, union status of transitioned employees,

geographic implications, services provided to employees and retention metrics after two years. Also describe the critical success factors associated with their project examples and explain how their approach resulted with a mutually beneficial result for employees and both organizations.

f) Demonstrated experience ensuring privacy protection and security in the management of government and other public sector information (Proponent Plus)

Each Proponent should describe its experience and that of each of its Subcontractors dealing with sensitive, confidential and personal information. Proponents should describe any quality assurance procedures and practices they had in place to provide protection and compliance for their own information and that of their clients, in particular that of government and other public sector entities. In addition, the Proponent must describe its experience complying with stringent privacy and security requirements similar to the Province's security policies and privacy legislation.

g) Demonstrated experience in designing and implementing complex economic models, engaging in long term commercial arrangements and experience in deal structuring (Proponent)

Using recent examples, each Proponent should describe their ability to address business issues, and then conceptualize and produce innovative economic models with the flexibility to handle changes in program deliverables over a long term commercial arrangement. Each Proponent should also describe their depth and breadth of experience in conceptualizing, negotiating and operating within each recent example.

Each Proponent is also required to describe their approach to sharing the risks and rewards associated with long term commercial arrangements and demonstrate, using recent examples, their success in maintaining a mutually beneficial relationship with clients. Each Proponent should provide project examples and describe how benefits were accelerated and project objectives were met or exceeded.

Using recent examples, similar or larger in financial size, scope and prospective change, each Proponent is required to demonstrate where they have successfully engaged in a long term (five or more years) commercial arrangement. For each recent example, each Proponent should describe the deal characteristics, such as, but not limited to: deal structure, financial size, length of term, type of pricing model, and any key features that illustrate the principles of flexibility and risk sharing.

h) Demonstrated experience managing complex project delivery with multiple stakeholder groups, and competing priorities (Proponent)

Each Proponent should describe past experience in managing and delivering complex projects. Experience should relate to services and projects similar (or greater) in complexity and scope to this opportunity.

Each Proponent should also outline critical challenges that were faced and how they were overcome.

i) **Demonstrated experience with organizational change management for complex projects (Proponent plus)**

Each Proponent should describe past experience in managing organizational change for complex projects. Experience should relate to services and projects similar (or greater) in complexity and size to the STMS Project Scope.

Each Proponent should also outline critical challenges that were faced and how they were overcome.

5.7.2.2 Capacity

a) **Corporate and financial capacity (Proponent)**

Each Proponent should describe where and when it has been engaged as a service provider with substantial financial obligation. Large scale public or private sector examples would be preferred and if possible, where the services were similar to the Scope of the Opportunity. Each Proponent should provide evidence of current financial stability and solvency.

b) **Demonstrate ability to assume and manage risk (Proponent)**

The Province is interested in the Proponent's experience in the management of risk including technology, implementation, operational, service delivery, financial, human resource, and investment risk. As the JSP Process contemplates a risk/reward sharing mechanism in the Final Contract, each Proponent is asked to demonstrate, using past project examples, where risks were assumed by the Proponent.

c) **Demonstrate capacity to design, transition, implement, and operate services within the Scope of the Opportunity (Proponent)**

Each Proponent is required to demonstrate their capacity to deliver, using current examples, (design, transition, implement, and operate) services of similar magnitude to the Scope of the Opportunity. Each Proponent should specifically demonstrate that they have the people, processes, and technology to deliver all components of the STMS Project Scope and the current infrastructure to deliver the mainframe services and the strategic transformation and hosting services. Each Proponent should also specifically demonstrate that they have the capacity to provide in the future the infrastructure necessary to deliver data centre facility services and the people, processes, technology, and infrastructure to deliver Potential In-Scope services as described in section 3.4.2.3.

5.7.2.3 Commitment

a) **Commitment of staff to engage in the JSP Process and STMS Project (All)**

The Province requires substantial commitment from Preferred Proponents that advance to later stages and phases, of the JSP Process and from the Successful Proponent into the first few years of the Final Contract.

Each Proponent should include the names and bios of individuals that will make up the Proponent's team as the JSP Process progresses from the Stage 2 Workshops through to the Contract Negotiation Phase. Each Proponent should describe the current roles and responsibilities of these individuals in the Proponent's organization, as well as the roles and responsibilities they will play

or assume in the JSP Process. Proponents should provide a project team organization chart.

In addition, each Proponent should describe how they propose to have individuals in key roles during the JSP Process continue to be involved during the early activities for the STMS Project after Final Contract execution.

b) Commitment to a long term relationship with the Province (Proponent)

Each Proponent should explain what they would do to ensure a successful relationship for all parties (e.g. the Service Provider, Province, BPS) and provide examples where they have been involved in a successful commercial relationship. Each Proponent is required to include information in their examples on any problems that were addressed in order to maintain the relationship.

c) Commitment to environmentally sustainable service delivery practices (Any)

Each Proponent should describe how they are committed to delivering services to clients in an environmentally sustainable manner.

5.7.2.4 High level concept

a) Provide a high level concept that addresses Workplace Hosting Services' business challenges, risks and objectives for the Scope of the Opportunity (Proponent)

Each Proponent should include in their Proposal a high level concept that briefly explains how the Proponent will address Workplace Hosting Services' business challenges, risks and objectives. In addition, Proponents should describe how the high level concept provides the needed flexibility and scalability to address future opportunities. Each Proponent should include the principles they will use to ensure the successful delivery of the Services over the term of the Final Contract and explain their use of Subcontractors, if any, to perform the Services.

5.7.3 References

Proponents are required to provide three (3) client references that are related to a service delivery operation of similar size to the Scope of the Opportunity. At least (1) one of the three (3) references should be directly related to hosting services and strategic transformation services, whether it is a reference of the Proponent or its Subcontractor as the case may be.

Proponents should detail the contact name, phone number, and the duration and description of the project or service delivery. Proponents will be notified by the Province before any of these references will be contacted, which may take place at any point during the JSP Process. In addition, the Province, at its sole option, may undertake further reference checks by contacting other corporate and project references in addition to the ones provided by the Proponent.

Appendix A. PROPOSAL COVERING LETTER

Letterhead or Proponent's name and address

Date

Ministry of Labour and Citizens' Services
Strategic Acquisitions and Technology Procurement Branch
c/o Reception Desk
2nd Floor, 563 Superior Street
Victoria, British Columbia, V8V 1T7
Attention: Pelle Agerup

Dear Sir/Madam:

Subject: Joint Solution Procurement Request for Proposal for the Strategic Transformation and Mainframe Services Project No. SATP-231 including any amendments (the "JSRFP").

The enclosed Proposal is submitted in response to the above-referenced JSRFP. Through submission of this Proposal, we agree to be bound by all of the terms and conditions of the JSRFP.

We have carefully read and examined the JSRFP and have conducted such other investigations as were prudent and reasonable in preparing the Proposal. We agree that subject to the terms and conditions of the JSRFP, we shall also be bound by statements and representations made in this Proposal.

Yours truly,

_____

Signature

Name: _____

Title: _____

Legal name of Proponent: _____

Date: _____

Appendix B. RECEIPT CONFIRMATION FORM

Strategic Transformation and Mainframe Services Project
Closing Date: July 26, 2007
Joint Solutions Request for Proposal No. SATP-231
Ministry of Labour and Citizens' Services

To receive any further information about this JSRFP please return this form to:

Attention: Pelle Agerup
Mail: Ministry of Labour and Citizens' Services
Strategic Acquisitions and Technology Procurement Branch
c/o Reception Desk
2nd Floor, 563 Superior Street
Victoria, British Columbia, V8V 1T7

Fax: (250) 356-0846
Email: pcadmin@gov.bc.ca

Company: _____

Street address: _____

City/Province: _____ **Postal Code:** _____

Mailing address if different: _____

_____

Phone number: _____ **Fax number:** _____

Contact person: _____

e-mail: _____

Unless it can be sent by fax or email, further correspondence about this JSRFP should be sent by courier collect as follows:

Courier collect.
Provide Courier name and account no: _____

_____

Signature: _____

Title: _____

Appendix C. JOINT SOLUTION DEFINITION AGREEMENT

The Preferred Proponents must enter into a Joint Solution Definition Agreement with the Province that will govern the actions of the Province and the Preferred Proponents during the Joint Solution Definition Phase, the Due Diligence & Negotiation Phase and the Contract Negotiation Phase. The Joint Solution Definition Agreement will include, but not be limited to, the provisions summarized below:

1. general representations, warranties and covenants;
2. conflict of interest provisions including representations and warranties in respect of conflicts and a requirement to implement a conflicts plan;
3. evaluation process including formation of the evaluation committee; certain evaluation criteria used to evaluate the Preferred Proponents; and the debriefing process;
4. the right of the Province to amend, modify or suspend the JSP Process or suspend or cancel negotiations with a Preferred Proponent;
5. right of the Province to designate an alternate Preferred Proponent;
6. obligation of Preferred Proponents to bear all of their own expenses;
7. restriction on lobbying and on any contact with Ministry or government personnel except as authorized by the Province;
8. due diligence covenants including certain rights of the Preferred Proponent to seek information from the Province and the right of the Province to consult outside references and obtain third party information regarding the Preferred Proponent;
9. the Province being under no obligation to enter into a Final Contract;
10. no obligation for the Final Contract to be based upon the JSRFP and the ability of the Province and the Preferred Proponent to enter into arrangements that exceed or only include part of the scope contemplated by the JSRFP;
11. duty of the Preferred Proponent to act in good faith throughout the JSP Process;
12. confidentiality provisions including (a) the Province agreeing to keep detailed Solutions of the Preferred Proponent confidential subject to reasonable exceptions in order to facilitate the JSP Process and subject to the Freedom of Information and Protection of Privacy Act; and (b) the parties agreeing on processes for information to be released in certain circumstances to other stakeholders;
13. privacy provisions;
14. intellectual property provisions including ownership rights, representations, warranties, indemnities and cross licensing provisions;
15. the term of the JSP Process, default provisions, termination rights and consequences of termination or breach;
16. a summary of certain terms that would be required to be included in the Final Contract including risk allocation, audit and reporting, limited force majeure, change control, service levels, default, privacy and confidentiality, proprietary rights, acceptance testing, termination services, dispute resolution and Province funding restrictions;

17. no representations or warranties from the Province; no liability of the Province for indirect or similar types of damages; and a limit of liability of the Province equal to the reasonable direct expenses incurred by the Preferred Proponent;
18. no liability for errors or inaccuracies of the Province;
19. no assignment right for the Preferred Proponent;
20. manner in which consortiums and their members are obligated to the Province; and
21. general provisions including notice, governing law, entire agreement, nature of relationship, survival and execution.

This Space Intentionally Left Blank

Appendix D. PRIVACY PROTECTION SCHEDULE

This Schedule forms part of the agreement between Her Majesty the Queen in right of the Province of British Columbia represented by_____ (the "Province") and _____ (the "Service Provider") respecting _____ (the "Agreement").

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Service Provider as a result of the Agreement or any previous agreement between the Province and the Service Provider dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Province to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Service Provider is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider may only collect or create personal information that is necessary for the performance of the Service Provider's obligations, or the exercise of the Service Provider's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider must tell an individual from whom the Service Provider collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Service Provider's collection of personal information.

Accuracy of personal information

6. The Service Provider must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Service Provider or the Province to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Service Provider receives a request for access to personal information from a person other than the Province, the Service Provider must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Service Provider to provide such access and, if the Province has advised the Service Provider of the name or title and contact information of an official of the Province to whom such requests are to be made, the Service Provider must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Province to correct or annotate any personal information, the Service Provider must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Province must advise the Service Provider of the date the correction request to which the direction relates was received by the Province in order that the Service Provider may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Service Provider must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Service Provider disclosed the information being corrected or annotated.

11. If the Service Provider receives a request for correction of personal information from a person other than the Province, the Service Provider must promptly advise the person to make the request to the Province and, if the Province has advised the Service Provider of the name or title and contact information of an official of the Province to whom such requests are to be made, the Service Provider must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Service Provider must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Province otherwise directs in writing, the Service Provider must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Service Provider must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Province otherwise directs in writing, the Service Provider may only use personal information if that use is:
    (a) for the performance of the Service Provider's obligations, or the exercise of the Service Provider's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Province otherwise directs in writing, the Service Provider may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of the Service Provider's obligations, or the exercise of the Service Provider's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Service Provider must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Service Provider, enter on the Service Provider's premises to inspect any personal information in the possession of the Service Provider or any of the Service Provider's information management policies or practices relevant

to its management of personal information or its compliance with this Schedule and the Service Provider must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Service Provider must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Service Provider as a service provider, including any applicable order of the commissioner under the Act; and
    (b) any direction given by the Province under this Schedule.

20. The Service Provider acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Service Provider does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Service Provider must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Province may have under the Agreement or otherwise at law, the Province may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Service Provider, terminate the Agreement by giving written notice of such termination to the Service Provider, upon any failure of the Service Provider to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Service Provider" in this Schedule includes any subcontractor or agent retained by the Service Provider to perform obligations under the Agreement and the Service Provider must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Service Provider in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Service Provider must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

This Space Intentionally Left Blank

Appendix E. TRANSPARENCY POLICY

The government of British Columbia is committed to the goals of openness and transparency in government procurement processes. The government of British Columbia supports the public's expectation of, and demand for, a higher level of disclosure about information relating to government business than it does for commercial relationships in the private sector.

While the government of British Columbia supports maximum disclosure of information regarding procurement processes, such disclosure must be done in a way that does not jeopardize the competitive process or government's negotiating position.

The intent of this policy is to increase openness and transparency by maximizing the proactive public disclosure of contract information, project summaries and performance measures related to alternative service delivery projects.

At the same time, this policy will ensure that the goal of maximum disclosure in the public interest is balanced against the need to protect commercially sensitive information of third parties and information which could harm the financial, economic or other interests of a public body or the government of British Columbia.

Scope

1. All ministries that are responsible for an alternative service delivery project must comply with this policy.
   1.1 For the purpose of this policy an "**alternative service delivery project**" is a complex alternative service delivery project involving the Alternative Service Delivery Secretariat and is designated as an alternative service delivery project by the Deputy Minister of the Ministry of Labour and Citizens' Services.

Direction to Negotiating Team

2. A ministry responsible for an alternative service delivery project must train and direct all members of its negotiating team on the application of this Transparency Policy.
3. A ministry responsible for an alternative service delivery project must direct its negotiating team to use the contract transparency format in negotiating the contract and the project summary template to describe the project. This format and template will ensure maximum disclosure of contract and project information.
   3.1 For the purpose of this policy "**contract**" means the Master Service Agreement or such other main agreement governing the alternative service delivery project.

Notice to Proponents

4. A ministry responsible for an alternative service delivery project must include in the procurement document a copy of this Transparency Policy and notice to proponents that the successful service provider will be expected to comply with the policy and to give all due consideration to the maximum public disclosure of contract and project information.

Public Disclosure of Contract and Other Information

5. A ministry responsible for an alternative service delivery project must proactively disclose to the public all provisions of the signed contract, subject to the exceptions set out in sections 9 and 10, below.

    5.1 Because disclosure of the provisions of the contract is presumed, the ministry must inform the parties to the contract that they have an obligation to identify when information that forms part of the contract may be commercially sensitive information that should be protected from disclosure.

    5.2 Where information is identified as excepted from public disclosure under section 9 or 10, the ministry must remove that excepted information and publicly disclose the remaining information.

6. A ministry responsible for an alternative service delivery project must disclose to the public a detailed summary of the project that includes project objectives, scope, rationale, vendor profiles, contract value, business cases, key changes that occurred during the procurement negotiation process, and key elements of the contract.

7. In disclosing information to the public under sections 5 and 6, a ministry responsible for an alternative service delivery project must use the contract transparency format for the alternative service delivery contract and the template for the project summary. These formats will ensure maximum disclosure of contract and project information.

8. A ministry responsible for an alternative service delivery project must disclose regular reports including, but not limited to:
    - performance reports based on the alternative service delivery project objectives and consistent with template guidelines established by the Alternative Service Delivery Secretariat; and
    - reports outlining additional contract and project information not originally contained in the project summary and as negotiated by the ministry and the service provider to increase project disclosure.

Protection for Commercially Sensitive Information

9. Before publicly disclosing the contract, a ministry responsible for an alternative service delivery project must remove from the contract, commercially sensitive information.

    9.1 For the purpose of this policy, "**commercially sensitive information**" means trade secrets or other confidential commercial, financial, labour relations, scientific or technical information of or about a third party that, if disclosed, could reasonably be expected to result in significant harm to the third party including, but not limited to:
    a) Information from competitive proposals;
    b) Economic models and detailed cost or pricing information (except for overall contract value);
    c) Corporate margins, including overhead or profit margins;
    d) Specific financial penalty amounts (not including a description of principles and penalty ranges);
    e) Names of key staff (other than corporate officers);
    f) Descriptions of proprietary technology, business processes, or methodologies, including ownership of intellectual property provisions;
    g) Productivity statistics (that could be deconstructed to provide competitive information such as number of staff proposed, etc.);
    h) Strategic clauses related to labour relations;
    i) Details of third party/subcontractor relationships (excluding names of material subcontractors, which should be released);
    j) Business development plans and targets;
    k) Service provider's corporate strategies;
    l) Disaster recovery and business continuity plan details;
    m) Limitations of liability, indemnities, and warranties; and
    n) Gainsharing provisions, terms and conditions around transition, security policies, practices and procedures.

Protection for Information Harmful to the Government

10. Before publicly disclosing the contract, a ministry responsible for an alternative service delivery project may remove information that, if disclosed, could reasonably be expected to harm the financial, economic, or other interests of the ministry or the government of British Columbia, including information the disclosure of which could reasonably be expected to harm the security or negotiating position of the ministry or the government of British Columbia.

Application of Policy to Existing Contracts

11. This policy applies to all new alternative service delivery projects, effective January 1, 2006. Where the contract for an alternative service delivery project was signed or largely negotiated prior to January 1, 2006, then the ministry responsible for the project must comply with only sections 6 and 8.

Appendix F. LIST OF WEBSITES IN JSRFP

Description	Website
Government Website	www.gov.bc.ca
Ministry of Labour and Citizens' Services	www.gov.bc.ca/lcs
Service plan for Ministry of Labour and Citizens' Services	http://www.bcbudget.gov.bc.ca/2007/sp/lcs/
Core Policy and Procedures Manual	http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm
Office of the Chief Information Officer, Privacy and Security Protection Policies	http://www.cio.gov.bc.ca/
Office of the Information Protection and Privacy Commissioner for British Columbia – Guidelines for Data Services Contracts.	http://www.oipcbc.org/advice/Guidelines-Data_services.pdf
FOIPPA and related policies and guidelines	http://www.mser.gov.bc.ca/privacyaccess/

Appendix G. CURRENT MAINFRAME ENVIRONMENT

Mainframe (MVS) service

The service broadly includes system management and reporting and data centre facility and operations services as outlined below:

System management and reporting:

- asset/inventory management;
- availability management;
- capacity management;
- change management;
- configuration management;
- performance management;
- problem management;
- recovery management;
- security management;
- service level management;
- system software management (e.g. currency, license mgt.); and
- workload management.

Data centre operations services:

- backup and recovery;
- communications connectivity (e.g. Netsol, TCP/IP, VTAM);
- database online services (DB2, IMS, CICS, MQ, SRS system);
- disaster recovery plan;
- document/print services;
- production control (batch, job scheduler);
- security controls (e.g. software, data centre);
- services support (e.g. services documentation);
- storage management (e.g. DASD, tape);
- system software support; and
- technical support – end users.

Mainframe (MVS) Software Base:

The current MVS service includes more than 100 software products from multiple vendors for the operating system, database subsystems and application development. A summary of the current software product list is provided below.

Vendor	Product Names
Allen Systems Group	Docutext Pro/JCL
BMC Software Inc	Delta Plex Extended Terminal Assist Plus LOAD PLUS for IMS Mainview® Tools Secondary Index Utility UltraOptIMS
Chicago Soft	MVS/QuickRef

Vendor	Product Names
Computer Associates Inc	AION Business Rules Expert Culprit Dads Plus for CICS Intertest for CICS MIA / MII SMR TSO Plus
Compuware Corporation	Abend-AID for IMS Abend-AID MVS CICS/Abend-AID/FX File-AID - for DB2, IMS w/DC options, MVS
Cybermation Inc	ESP / ESP Encore
Fischer International Systems	IOF/TSO
IBM	z/OS ADF ASF CICS TS COBOL for OS/390 & VM DB2 UDB DCF / DLF IMS, IMS Utilities IMS/ESA BTS Image Plus InfoPrint Server MQ Series NCP Netview PL/I for MVS & VM PPFA PSF QMF SDF SDSF Security Server (RACF) TSO Unix System Services (e.g. Java, SecureFTP, SecureLDAP) VAG VPS / DRS
Innovation Data Processing	FATS/FATAR FDR, FDR-Crypt
Levi, Ray, Shoup Inc.	VPS VPS / TCPIP DRS
MacKinney Systems	CICS Message
Merrill Consultants	MXG
Mobius Management Systems	ViewDirect Document Direct for Internet
MVS Solutions Inc	Thruput Manager – JBS, DCS
Open Software Technologies	REXXtools MVS
Pathlore Software	Preference
SAS Institute	SAS

Vendor	Product Names
Software Engineering of America	PDSFAST
SPSS Inc.	SPSS Stat
SYNCSORT Inc	Syncsort for z/OS PROC/Syncsort z/OS

Appendix H. ICBC DATA CENTRE REQUIREMENTS

Data Centre Requirements

Background

The ICBC data centre located on the 6th floor at 151 West Esplanade in North Vancouver was built in the early 1980s as part of the Corporation's head office building. The data centre facility was designed for mainframes that had different environmental requirements than current platforms and it is reaching the end of its design life. It would require extensive renovating if it were to be used beyond three years into the future. Shortcomings of the existing data centre include a floor that is structurally inadequate to support modern equipment, recurrent roof leaks, and heating, ventilating and air conditioning inadequate for future equipment needs. The Information Technology (IT) Infrastructure group has mitigated risk to this point, however these measures cannot provide the reliability required to support the Corporation's critical business systems and sustain the organization in the long term.

Over the years, the ICBC data centre has evolved from being of operational importance to being a strategic corporate asset, with business requiring it to be available 24x7x365, and strategic business decisions being dependent on its ability to change and adapt. The datacentre now represents a competitive advantage to ICBC, servicing custom-designed broker-customer sales transactions, and securing a vital asset, the store of claims and insurance data.

The data centre facility must be able to adapt over the years, and it must be able to do this reliably, without disrupting business operations. The data centre supports claims offices with extended hours, 7 days a week insurance sales, 24x7 customer-facing call centre operations, and customers accessing web applications at any time.

Objectives

ICBC's Data Centre initiative is driven by the goal to:

Ensure a reliable data centre facility that will sustain the Corporation for the foreseeable future.

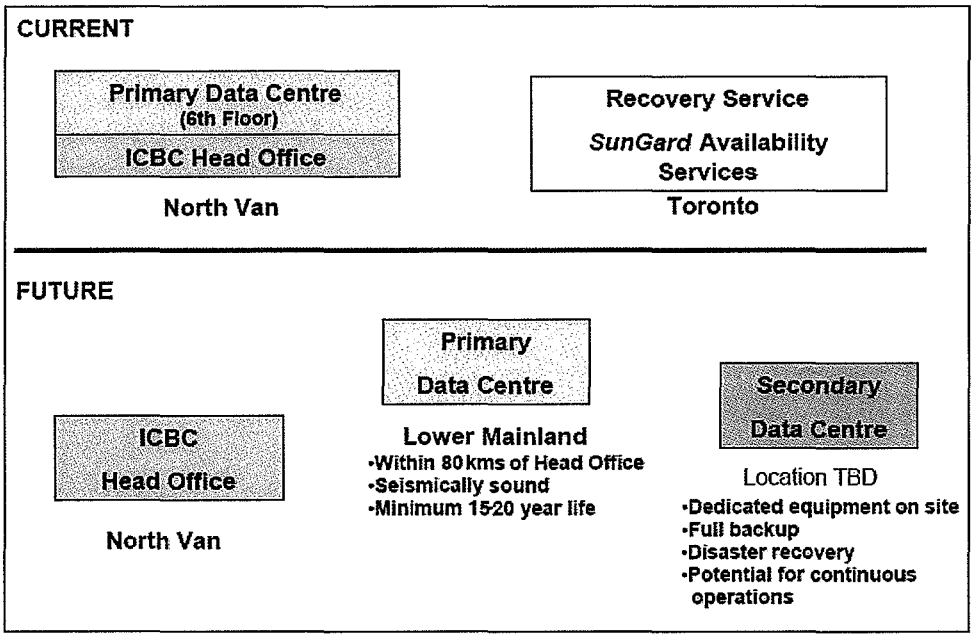
To attain this goal, four key objectives have been identified:

1.	Long-term Facility Requirements	Satisfy the facility requirements for a data centre to sustain the organization for a 15-20 year lifespan.
2.	Operational by End of 2010	Implement data centre operations in the new facility by the end of 2010.
3.	Cost/Benefit	Ensure the data centre solution is cost effective.
4.	Risk	Ensure that minimizing risk is a key consideration in developing the solution.

ICBC Data Centre – Current and Future

As discussed, ICBC's primary data centre is located in the North Vancouver head office. Secondary data centre services are provided by SunGard Availability Services in Toronto, Ontario. ICBC is currently assessing its overall processing needs including those of two of its critical systems hosted on the Workplace Technology Services (formerly Common IT Services (CITS)) mainframe in Victoria.

ICBC's vision for the future is represented by the following diagram.



SUMMARY OF REQUIREMENTS

Reliability Level

Data centers with a higher reliability level have redundancy built into them and will cost more. ICBC uses the Brunspak reliability levels criteria and have opted for a Level 7 (Tier II Uptime Institute) with the ability to move to a level 8 (Tier III Uptime Institute) if required. Building redundancy into data centers at the outset is more cost effective than trying to upgrade them later.

The following table summarizes the ICBC's Data Centre requirements

Requirements	Preference High/Low
Implement data centre operations in the new facility by the end of 2010.	H
Facility can house Data Centre for next 15 years at a	H

Requirements	Preference High/Low
minimum	
Location	
1. Outside 200 year floodplain	H
2. Seismically sound area	H
3. Not located near sources of vibration	H
4. Near good public transportation network (primary)	H
5. No more than 80 Km from Esplanade Head Office (primary)	H
6. No more than a one hour commute from Esplanade Head Office (primary)	H
7. Near two major communication carriers	L
8. Crime rate should be low	L
Space	
1. Raised Floor area of 10,000 Sq. Ft.(primary data centre)	H
2. Raised Floor area of 4,000 Sq. Ft. (second data centre)	H
3. Office Space of 6,000 Sq. Ft. (primary)	H
4. Infrastructure area	H
5. Build out space	L
Architectural	
1. Raised Floor Loading of 300 lbs/Sq. Ft.	H
2. Minimum height of 15 ft. from slab to slab	H
3. Data Centre located in single story building at ground level	H
4. Raised floor height of 30"	H
Electrical	
Power - 2000kva unit substation	H
UPS – 2 x 75kv	H
Power 75w per sq ft	H
Backup Generator – 1 x 1500kv	H
Cooling	
190 tons of cooling required for 75w per sq ft	H

SCHEDULE 41

PROVINCE SHARED INFRASTRUCTURE

1. **Province Shared Infrastructure.** This Schedule identifies specific Province Shared Infrastructure, that the Service Provider will use in the delivery of, or performance of, the Services for the Province as follows:

(a) **Use of SPAN/BC**

(i) **Remote Monitoring** - The Province will provide the Service Provider with access through SPAN/BC to in-scope servers located in other than data centre facilities, in order to allow Service Provider to monitor those servers. The monitoring consists of very low volume network traffic from the Service Provider monitoring network connections into SPAN/BC to each of the remote sites.

(ii) **Remote Server Backups** - The Province will provide adequate network connectivity to remote site and capacity to each server location, other than data centres, to ensure that the required backup of each server can continue to occur within the backup window.

(iii) **Log File Collection** - S. 15

S. 15

(b) **Active Directory ("AD")** - The Province will provide the Service Provider with use of or support from the existing Government of British Columbia Active Directory (for example, IDIR, TIDIR, etc.) services in the delivery of its managed hosting responsibilities. These services include:

(i) the provision of privileged IDs for the Service Provider authorized service Personnel to support midrange servers;

(ii) the Service Provider role in the provision of privileged IDs to the Province "application owners";

(iii) use of the Distributed File System ("DFS"), hosted and maintained by Active Directory, for providing a unified file directory structure, required by the Shared File Print ("SFP") service;

(iv) the Service Providers role in maintaining logon scripts for provincial users; and

(v) access to Active Directory Organizational Units ("OUs") for the management of midrange servers.

(c) **Anti-Virus and Malware** - The Service Provider S. 15

S. 15

(d) **Client Access Management Infrastructure and Services** - The Service Provider requires that WTS continue to provide router, Access Control List, and firewall provisioning, management and administration services for both the Service Provider and end user access to WTS server infrastructure in WTS or other Province facilities. As servers are migrated to the STMS data centres, the Service Provider will manage firewalls and administer firewall rules, data centre network devices, and server user privileges for those devices located at STMS data centres, but will not undertake management of the Active Directory function.

(e) **Province Provided Internet Services** – The Province will allow the Service Provider to utilize internet services for S. 15

S. 15

(f) **Third Party Gateways** - The Service Provider Service Delivery Management network connections to SPAN/BC, at the Province's S. 15

S. 15 will be enabled by the Province. The Province will allow the Service Provider to install routers at those sites and the Province will provide and manage access firewalls in accordance with the Province Third Party Gateway standards. The Province will supply the Service Provider with network access to the remote and data centre server and storage infrastructure by ensuring that all firewalls and router configurations support such access.

(g) **Exchange Services** - The Province will allow the Service Provider to utilize the Province Exchange mail service to deliver alerts, notifications and escalation notifications (as such number of shared IDs are limited in accordance with the Services Management SOW).

(h) **Service Management Infrastructure** - Recognizing that the Province Ordering System, ITIMS Remedy, eHealth and BizTalk are used by the Province for purposes other than supporting the WHS hosting services, this section addresses shared service management infrastructure such as the Client Service Centre ITIMS system.

In the delivery of the Service Provider service management services, the Service Provider requires integration with and support from the Province Ordering System, ITIMS, and integration services with BizTalk. The delivery of Request, Change, Incident, and Problem management services will be established based on

the existing Province infrastructure and processes implemented and executed using Province Ordering System for Request Management and ITIMS for the recording and management of Incident, Problem, and Change. S. 15

S. 15

The Service Provider Service Management Services described in the Services Management SOW will be dependant upon the ongoing delivery of Province requests, incidents, problem and change management information from existing Province services. The Service Provider will replace WHS as the receiver of service management transactions/information without any significant change to the existing Client Service Centre and Province Ordering System services with the exception of automated bridging. The automated bridging of ITIMS initiated incident tickets to the Service Provider will be required to support service management operations. The Province will provide all manual process flow changes from ITIMS or Province Ordering System as agreed to and documented.

(i) **Data Centre Services** - Existing Province Data Centres, Remote Infrastructure Server Locations and the Remote Application Server Locations as set out in Schedule 8.

(j) **Transition Period** - Workstations, prior shared file print infrastructure, remote infrastructure

2. The Province Shared Infrastructure referred to in this Schedule 41 shall be operated and maintained by the Province as a Province retained cost, and accordingly, the Province will not charge a use fee to the Service Provider for the use of the Province Shared Infrastructure Schedule as set forth above.

SCHEDULE 42

DESIGNATED ARBITRATORS

At issue for Inquiry

With respect to the list of Designated Arbitrators set forth above, the Parties acknowledge and agree that once a Designated Arbitrator has acted in connection with a Dispute, such Designated Arbitrator will not be selected to arbitrate another Dispute until:

(a) all the other candidates have acted on at least one Dispute;
(b) the individual is the only candidate available to act on the particular Dispute; or
(c) the Parties both consent.

SCHEDULE 43

SOFTWARE RESPONSIBILITY TABLE

See attached

Code	Type of Software	Definition
PLicensed	Province Licensed Software	means the Third Party Software for which the Province has a license to use in the Province of British Columbia and which the Province has the right to authorize the Service Provider to use in the manner specified in Section 19.9 (*Use of Province Licensed Software*), including the Third Party Software identified as "Province Licensed Software" in Schedule 43 (*Software Responsibility Table*).
PProprietary	Province Proprietary Software	means the Software owned by the Province, including object and source code versions, and any Documentation and any Modifications or interfaces relating to the foregoing created by or on behalf of the Province from time to time, but excluding Third Party Software, which is identified as "Province Proprietary Software" in Schedule 43 (*Software Responsibility Table*) and may otherwise be notified in writing by the Province to the Service Provider from time to time.
SP Leverage	SP Leveraged Software	means the SP Licensed Software that is excluded from the provisions of Section 19.12 (*Assignment of SP Licensed Software*) and is identified as "SP Licensed Software" in Schedule 43 (*Software Responsibility Table*). [NOTE - EDS has identified this as being IBM, Computer Associates and McAfee.]
SP Licensed	SP Licensed Software	means the Third Party Software for which the Service Provider has a license to use in the Province of British Columbia and which the Service Provider has the right to authorize the Province to use in the manner specified in Section 19.11 (*Use of SP Licensed Software*), including the Third Party Software identified as "SP Licensed Software" in Schedule 43 (*Software Responsibility Table*).

Code	Type of Software	Definition
SP Proprietary	SP Proprietary Software	means the Software owned by the Service Provider on the Hand-Over Date, or which it develops or acquires after the Hand-Over Date independent of this Agreement, including object and source code versions, Documentation and any Modifications or interfaces relating to the foregoing, created by or on behalf of the Service Provider from time to time, and that is used in the provision of the Services, and includes SP Affiliate Bespoke Software and the Software identified as "SP Proprietary Software" in Schedule 43 (*Software Responsibility Table*); for the purposes of clarity, SP Proprietary Software excludes Province Proprietary Software, SP Affiliate Commercial Software or Third Party Software.

APPENDIX A - MAINFRAME SYSTEM SOFTWARE

Third party	Software	Type of Software	Transferable at end of Term	Assignable	Additional Notes	Responsible for S/W	Transfer Fee at end of Term
Appendix A.1.1 Standard Software - The Service Provider Provided Base Software							
Computer Associates	CA-CCS CA-CCS S. 15 CA-Vantage Multi Image Integrity SMR	SP Leveraged Software	No	Software is licensed under an annual term license. License is not transferable.		EDS	N/A
IBM	CICS S. 15 DB2 UDB S. 15 S. 15 Ent COBOL S. 15 ICKDSF JAVA S. 15 REXX Library S. 15 SD/2 HAS S. 15 SMP/E System Automation WebSphere MQ WebSphere MQ S. 15 z/OS Base z/OS Opt z/OS Opt z/OS Opt z/OS Opt S. 15 z/OS Opt z/OS Opt IMS/ESA S. 15	SP Leveraged Software	No	S/W is licensed under a term license; therefore S/W License can not be transferred over to the customer.	S/W can also be licensed under a Perpetual License; Perpetual Licenses can be transferred over to the customer after 24 months under EDS' name System Automation product has EDS IP wrapped around it and could reside in this sub section or A.1.2. Regardless of which Appendix, neither the software nor the IP is transferable.	EDS	N/A
Innovation	FATS/FATAR	SP Licensed Software	Yes	The S/W license can be transferred but it is restricted for use by the Province only.		EDS	No Fee
STK	ExLM HSC_STK_Atl	SP Licensed Software	Yes	Yes		EDS	No Fee
Syncsort Incorporated	Syncsort S. 15	SP Licensed Software	Yes	Yes. A template needs to be filled out in order to complete the transfer		EDS	No Fee
Appendix A.1.2 Standard Software - The Service Provider Developed Software							
	ATRM CHARMS CICS CICS S. 15						

EDS	CICS S. 15 S. 15 Crystal Data Set Update and Display Date Manipulation DB2 DB2 S. 15 Device Scanning System Document Facility EDF eSMS FZA S. 15 GRS Enqueue Display Hold Job S. 15 IMS IMS S. 15 IPCS Interface S. 15 JCS2 S. 15 JES2 Extensions S. 15 MOM MPF Exits S. 15 Multi DB2 MVS SMF Exits MVS Utilities JES2 MVD3300 MXI NPL Network Procedure Language Online Notification EON PAM PDS S. 15 Problem Change Collection Tool PCCT PRO-J QueryAid for DB2 Reusable Programs Reusable Subs & Macros SAM SCM S. 15 Service Excellence Dashboard ShowMVS SME SOS SP Tools S. 15 Standard TSO S. 15 Transparent Loaders Unicenter CA S. 15 WPAXGET S. 15	SP Proprietary Software	No	S/W not transferable as these products are the intellectual property of EDS		EDS	N/A

Appendix A 2.1 - Non-Standard Software - The Service Provider Provided WTS Paid Software							
BMC Software	CMF MONITOR Delta Plus ETA Plus S. 15 IMS MAINVIEW MAINVIEW MAINVIEW MAINVIEW MAINVIEW MAINVIEW S. 15 MAINVIEW MAINVIEW MAINVIEW MAINVIEW UltraOpt/IMS	S. 15 Licensed Software	Yes	The S/W License can be transferred but it is restricted for use by the Province only.	Transfer Fee = 10% of List Price of Licenses at the moment of the transfer	EDS	Yes
Chicago Soft Inc	MVS/QuickRef	S. 15 Licensed Software	N/A	Not Applicable as S/W needs to be licensed under the Province's name.	S/W vendor will grant EDS access to the S/W for a specified period of time	Province	N/A
Computer Associates	Aion/DS AllFusion CA-Intertest for CICS BATCH PROCESSOR Culprit MVS ESP ESP Encore PDSMAN XCOM XMANAGER	S. 15 Licensed Software	No	Software is licensed under an annual term license. License is not transferable.		EDS	N/A
	AFP Font Collection ASF - Doc Composition Feature BARCODE Batchpipes CCCA S. 15 DCF DCF DLF Debug Tool S. 15 EnterpriseS. 15 FAF/CICS FAF/IMS Fonts - DATA1 BBOX Fonts - DATA1 UBOX Fonts - Son S Ser HD3820 Fonts - Son Sans 3820 Fonts - Son Serif 3820 Fonts - Son Serif HD3820						

IBM	Host Command Facility IMS High Performance IMS High Performance S. 15 IMS Library Integrity Utilities S. 15 IMS/ADF II InfoPrint Transforms IODM NCP NCP NCP S. 15 NCP NCP Netview S. 15 OGI S. 15 PL/I S. 15 PPFA S. 15 S. 15 PSF PSF PSF S. 15 PSF S. 15 MVS MVS S. 15 MVS MFS VisualAge Gen Server XML Toolkit z/OS Opt z/OS Opt z/OS Opt z/OS Opt z/OS Opt z/OS Opt S. 15 z/OS Opt z/OS Opt z/OS Opt z/OS Opt	SP Developed Software	No	S/W is licensed under a term license; therefore S/W License can not be transferred over to the customer.	S/W can also be licensed under a Perpetual License; Perpetual Licenses can be transferred over to the customer after 24 months under EDS' name	EDS	N/A
S. 15		SP Licensed Software	Yes	The S/W license can be transferred but it is restricted for use by the Province only.		EDS	No Fee
SAS Institute (Canada) Inc.	SAS SAS SAS S. 15 SAS SAS	SP Licensed Software	Yes	Yes	The Province will be required to execute a S/W License Agreement (if no one is in place) and execute an Outsourcing Amendment	EDS	No Fee

	SAS S. 15						
Syncsort Incorporated	PROC Sync Sort MVS	S/W Licensed to Province	Yes	Yes. A template needs to be filled out in order to complete the transfer		EDS	No Fee
Appendix A 2.2 - Non-Standard Software - WTS Provided Software							
Allen Systems Group	Docutext Pro S. 15 ViewDirect for MVS	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Canada Post - CPC Data Licensing	Directories of Postal Codes	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Compuware Corporation	Abend Abend S. 15 ECC ECC ECC S. 15 ECC S. 15 MS Fileaid FileAi S. 15 Fileaid/IMS Fileaid/IMS S. 15 Fileaid/MVS Fileaid/SPF Fileaid/XE	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Fischer International Systems	IOF	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Innovation	FDR	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Levi, Ray & Shoup, Inc.	DRS VPS VPS / TCPIP	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Merrill Consultants	MXG	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	EDS may be required to acquire a S/W License in addition to the S/W License hold by the Province	Province	N/A
MVS Solutions Inc.	Thruput Manager Thruput Manager Thruput Manager S. 15	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Open Software Technologies Inc.	Rexx Tools Rexx Tools S. 15 REXXtools / MVS	Province's Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A

Pathlore Software Corporation	Preference Library & Preference W/Options	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Prism Data Services	Dr. Q	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Software Engineering of America	PDSFAST	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
SPSS Inc.	SPSS STAT	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Relational Architects	RAI Launch Express	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Appendix A2.3 - Non-Standard Software - WTS Developed Software							
Province	S. 15 Service Request System (SRS) Province Provided Usermods and Exits	Province Proprietary Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A

Schedule B1 - Midrange - Province Owned Servers

Servers used to host the Province Applications (dedicated and servers used for shared services such as SFP)

Third party	Software	[redacted]	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
[redacted]	Remainder all Province Software - Software & Licenses Catch All	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
BMC	Remedy Action Request System	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	Software is used for several timekeeping and change purposes (Hosting, ITIMS), Network Node Registry (IT Service Management) and other related services	Province	N/A
Emulex	HBAnywhere	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
S. 15		[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	See Schedule B2 for reuse of these licenses on EDS servers as Province server assets diminish through transformation.	Province	N/A
Computer Associates	S. 15	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	S. 15	Province	N/A
Computer Associates	eHealth - only until EDS tools in place (6 months) S. 15	[redacted]	N/A	No. The S/W is licensed under an annual term license and it's not transferable	S. 15	Province	N/A
Microsoft	Windows Server operating system (all versions) windows Server 2003 windows server 2008 Microsoft KMS – Key Management Service - allows a single product key to be used for multiple installations (WTS utility servers) Microsoft Operations Manager (MOM) or Service Centre Operations Manager (SCO) SharePoint (used in shared web services) Microsoft SQL server – implementation of a relational database management system S. 15 Microsoft AIS/Radius S. 15 S. 15 Microsoft NLBS – a network load balancing and clustering implementation	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name. Executing an Enrolment Agreement between the Province, EDS and MS is required.Products will be procured at the Prices in the existing Province / MS agreement.	EDS to procure/leverage EDS' existing support (i.e. "Premier Support") arrangement with Microsoft	Province	N/A
Entrust Inc.	Entrust S. 15	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	AES Managed. Province to retain ownership of the Certs	Province	N/A
HP	HP hardware management tools	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	EDS Tools (automation) Agent	Province	N/A
Oracle	Oracle Management tools	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	AES unitilized Oracle tools for DBA services	Province	N/A
Webalizer	Webalizer	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	GNU General Public License	Province	N/A
Double-Take Software, Inc	DoubleTake	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Sun	SunOne Directory Server	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
IBM	WebShere	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	AES managed WebSphere	Province	N/A
Red Hat, Inc.	All required Redhat OS and tool licensing	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
software ag	WebMethods	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	Data broker used by AES	Province	N/A
Objective Development Softw	Sharity (SMB/CIFS client for Environment Servers)	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
VMware	All required VMware OS and tool licensing (including VMware Enterprise Suite & VMware Virtual Control Centre)	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Guidance	EnCase Enterprise	[redacted]	N/A	Not Applicable as S/W License remains under the Province's name.	Must determine if this software will be installed on existing server infrastructure	Province	N/A
HP	HP hardware management tools OPSware	[redacted]	Yes	Yes		Province	No Fee

Schedule B2 - Midrange - EDS Owned Servers

Servers used to host the Province business applications (dedicated and servers used for shared services such as SFP)
Where EDS software can be transferred back to the Province, the Province will be responsible for the establishment of maintenance/support agreements with the software Vendor.

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
Adobe	Adobe Acrobat Reader	SP Licensed Software	Yes	Yes as per Adobe Software License agreement found at Adobe website.	S/W License is free of charge	EDS	No Fee
McAfee	McAfee Virus Scan	SP Leveraged Software	No	Not assignable as S/W is licensed under an annual term license. If a perpetual license was acquired, the S/W could be assigned back to the Province	Incremental new licenses above the existing Province License quantity.	EDS	N/A
McAfee	McAfee Virus Scan	Province Licensed Software	N/A	Not Applicable as S/W License are to be acquired under the Province's name.	Re-use of existing Province Licenses	Province	N/A
IBM	All required IBM OS and tool licensing	SP Licensed Software	Yes	Yes, S/W License needs to be under EDS's name minimum 24 months		EDS	No Fee
SUN	All required SUN Solaris and tool licensing SUN-ILOM (Integrated Light Out Management) agent	SP Licensed Software	Yes	Yes, EDS may transfer S/W back to the end user customer at no charge to EDS or EDS' customer.		EDS	No Fee
Winzip	Winzip	Province Licensed Software	N/A	Not Applicable as S/W License are to be acquired under the Province's name.	EDS can purchase the License on behalf of the customer, but the license should be registered under the client's name. EDS can act as the outsourcer and administer the license for them.	EDS (Under Province's name)	N/A
Microsoft	All required Microsoft OS and tool licensing Microsoft SQL	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name. Executing an Enrolment Agreement between the Province, EDS and MSF is required.	Province to Procure using existing GSAM process under existing MS contract	Province	N/A
Freeware	S. 15	SP Licensed Software	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Software may or may not be transferable, however due the nature of the License free or charge, no transfer of license may be required as the customer may download any required license free of charge. Will be the Province's responsabaility obtaining required licenses at the end of the deal.			N/A

Oracle	Oracle RDBMS	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Citrix	Citrix	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
HP	HP hardware management tools OPSware	SP Licensed Software	Yes	Yes		EDS	No Fee
CA	Siteminder	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	Province Owned for Authentication	Province	N/A
CA	CA Unicenter S. 15 S. 15	SP Licensed Software	No	No. The S/W is licensed under an annual term license and it's not transferable		EDS	N/A
Symantec Corporation	Veritas Veritas S. 15 S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
EMC	Powerpath	SP Licensed Software	Yes	Yes		EDS	No Fee
S. 15		Province Licensed	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
VMware	All required VMware OS and tool licensing (including VMware Enterprise Suite & VMware Virtual Control Centre)	SP Licensed Software	Yes	Yes		EDS	No Fee

Schedule B3 - Midrange - EDS Owned Tool Servers

Servers used solely to enable EDS to deliver hosting services

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
IBM	IBM Tivoli Network Monitoring IP (TNM-IP) V3.7	SP Licensed Software	Yes	Yes, S/W License needs to be under EDS's name minimum 24 months		EDS	No Fee
Microsoft	Windows Server operating system (all versions) windows Server 2003 windows server 2008 Microsoft KMS – Key Management Service - allows a single product key to be used for multiple installations (WTS utility servers) Microsoft Operations Manager (MOM) or Service Centre Operations Manager (SCO) SharePoint (used in shared web services) Microsoft SQL server – implementation of a relational database management system S. 15 Microsoft AIS/Radius S. 15 S. 15 Microsoft NLBS – a network load balancing and clustering implementation	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name. Executing an Enrolment Agreement between the Province, EDS and MSF is required.	Province to purchase under existing MS contract and process using GSAM	Province	N/A
NetQOS	Application/Service monitoring software	SP Licensed Software	Yes	Yes, intention to transfer the S/W Licenses needs to be communicted to the publisher at the time of the acquisition of the Licenses		EDS	No Fee
EMC	Application Discovery Manager	SP Licensed Software	No	Not transferable to Province due to vendor restrictions.		EDS	N/A
VMWare	VMWare agnents	SP Licensed Software	Yes	Yes		EDS	No Fee
Computer Associates	CA Concord eHealth S. 15 S. 15 CA Job Management S. 15 S. 15	SP Licensed Software	No	No. The S/W is licensed under an annual term		EDS	N/A

Computer Associates	CA Management for Web Servers S. 15 CA Unicenter S. 15 S. 15	[redacted]	No	license and it's not transferable		[redacted]	N/A
McAfee	McAfee Anti Virus	SP Licensed Software	No	Not assignable as S/W is licensed under an annual term license. If a perpetual license was acquired, the S/W could be assigned back to the Province	For Anti Virus license requirements above the Province's current quantity	EDS	N/A
Symantec Corporation	Veritas Veritas S. 15 S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Citrix	Citrix – used for EAS/EDS access to management rail.	SP Licensed Software	Yes	Yes, intention to transfer the S/W Licenses needs to be communicted to the publisher at the time of the acquisition of the Licenses		EDS	No Fee
RSA	RSA Authentication Manager S. 15 S. 15 RSA Auth Mgr Maint S. 15	SP Licensed Software	Yes	Yes, transferability needs to be agreed upon at the moment of executing the initial License Agreement. Transfer cost may apply		EDS	No Fee
SUN	All required SUN Solaris and tool licensing SUN-ILOM (Integrated Light Out Management) agent	SP Licensed Software	Yes	Yes, EDS may transfer S/W back to the end user customer at no charge to EDS or EDS' customer.		EDS	No Fee
HP	HP hardware management tools OPSware	SP Licensed Software	Yes	Yes		EDS	No Fee

Schedule C1 - Storage and Back Up - Province Owned Infrastructure - Operating Software

Exisiting Province Products in support of storage and back up services

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
EMC	EMC ControlCenter Backup Advisor Active Engine Failover S. 15 NetBackup Media Mgr Software Option RTU Centera basic S. 15 NAVI MGR CX3 S. 15 NAVI ENTERPRISE MEDIA NAVI AGENT WINDOWS MEDIA Windows Software Utilities PPATH SES. 15 SYMM OPT S. 15 SYMM OPT BASE LICENSE SECURE REMOTE SUPPRT GW SMC S. 15 SOFTWARE KIT EMC S. 15 Sym pkg S. 15 NEW SYMM PKG S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Sun	Solaris	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
Symantec	NetBackup NetBackup NetBackup S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A

Schedule C2 - Storage and Back Up - EDS Owned Infrastructure - Operating Software

Exisiting EDS Products in support of storage and back up services

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
EMC	EMC ControlCenter Backup Advisor Active Engine Failover S. 15 NetBackup Media Mgr S. 15 RTU Centera basic S. 15 NAVI MGR CX3 S. 15 NAVI ENTERPRISE MEDIA NAVI AGENT WINDOWS MEDIA Windows Software Utilities PPATH SE SYM SYMM OPT S. 15 SYMM OPT BASE LICENSE SECURE REMOTE SUPPRT GW SMC S. 15 SOFTWARE KIT EMC S. 15 Sym pkg S. 15 NEW SYMM PKG S. 15	SP Licensed Software	Yes	Yes, EDS may transfer S/W back to the end user customer at no charge to EDS or EDS' customer.	Province required to provide ongoing maintenance/support contract after handover	EDS	No Fee
EMC	DiskXtender SRDF Point in Time	SP Licensed Software	Yes	Optional Services that if required will be purchased by EDS and are transferable		EDS	No Fee
Sun	ACSLS server Key management server Solaris	SP Licensed Software	Yes	Yes, EDS may transfer S/W back to the end user customer at no charge to EDS or EDS' customer.		EDS	No Fee
Symantec	NetBackup NetBackup NetBackup S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.		Province	N/A
CA	CA Job Management S. 15 S. 15	SP Leveraged Software	No	No Software is licensed under an annual term license and it's not transferable		EDS	N/A

Schedule D1 - Network

Network Appliance Software, tools and network security products

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
Computer Associates	CA Concord eHealth S. 15	SP Leveraged Software	No	No. The S/W is licensed under an annual term license and it's not transferable		EDS	N/A
IBM	Netcool Netcool NetCool S. 15 Netcool Netcool	SP Leveraged Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
IBM	Tivoli Network Monitor S. 15	SP Licensed Software	Yes	Yes, S/W License needs to be under EDS's name minimum 24 months		EDS	No Fee
NetIQ	App Manager	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
NetQOS	Performance Analyzer SuperAgent	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not		EDS	N/A
Cisco	Ciscoconf CiscoWorks RME Cisco WCS	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
HP	Peregrine Service Center OpsWare Network Automation System (NAS) HP Openview	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
Visionael	Visionael	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
IPTAS	IPTAS	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
Master Data List	Master Data list	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
Clarus	Clarus	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A
VoiceRite	VoiceRite	SP Licensed Software	No	No. The S/W is licensed by EDS and leveraged for use by other clients; that's why it is not transferable		EDS	N/A

Note: This S/W relates to EDS provided software as it relates to EDS new datacenter

Schedule E1 - Security

Security Software

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
Tripwire S. 15	S. 15	SP Licensed Software	Yes	Yes, transferability needs to be agreed upon at the moment of executing the initial License Agreement. Transfer cost may apply		EDS	No Fee
McAfee S. 15		SP Licensed Software	No	No if software is licensed under an annual term license. If license is under perpetual term it can be transferred to the customer		EDS	N/A
RSA S. 15		SP Licensed Software	Yes	Yes, transferability needs to be agreed upon at the moment of executing the initial License Agreement. Transfer cost may apply		EDS	No Fee
Bluecoat S. 15		SP Licensed Software	Yes	If the product is under maintenance and still supported by the manufacturer, it can be transferred over to the customer		EDS	No Fee
Crossbeam		SP Licensed Software	Yes	Yes, it can be transferred. However, we are more talking about hardware (like a Cisco router for example) so you can't just transferred the software. We only require formal writing approval prior to the transfer.	Annual Support Agreements No additional software on these firewalls other than Check Point software below.	EDS	No Fee
Check Point		SP Licensed Software	Yes	Yes, as long as the licenses are intended to have continued use with the client. If the client attempts to resell the licenses, there is an issue. This is completed by using an online tool	This is done by accessing http://usercenter.checkpoint.com. I also have a Step-By-Step guide with more explanations	EDS	No Fee
Seccuris		SP Licensed Software	No	NO - this is Seccuris IP or leveraged Seccuris solution	PCI Security Mgmt	EDS	N/A
RSA S. 15		SP Licensed Software	Yes	Yes, transferability needs to be agreed upon at the moment of executing the initial License Agreement. Transfer cost may apply	Optional Service	EDS	No Fee

Schedule F1 - Data Centre

Data Centre services and reporting tools

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
Q9 Control Panel	- General account management including administration of customer contacts, security access and emergency escalation procedures - Bandwidth reports that display bandwidth utilization in 5-minute averages with the 95th percentile highlighted to give a clear indication of usage for the current month. Additional weekly, monthly and yearly graphs chart historical utilization - Bandwidth monitoring with customizable thresholds alarms - Q9 network status reports - Protocol monitoring (customer-configured monitoring for PING, HTTP, FTP, SMTP, POP3) with automatic issue notification ' - Creation and management of support tickets - Power monitoring (co-location customers only – for more information, refer to the Q9 Physical Space service description document)	SP Leveraged Software	No	No – Q9 IP		EDS	N/A

Schedule G1 - Service Management

Hosting Service Management Suite

Third party	Software	Type of Software	Transfer Status	Fee
EDS	Digital Workflow EEIB (Bridge)	SP Proprietary Software	No	Individual components (Peregrine) can be licensed from HP
	eSLR S. 15	SP Proprietary Software	No	
	Reporting – MS Reporting and Excel	SP Proprietary Software	Yes	None – included in MS product suite
	Global Billing S. 15	SP Proprietary Software	No	
	STMS Portal	SP Proprietary Software	Yes	None – included in MS product suite
	Service Excellence Portal	SP Proprietary Software	No	

Schedule H1 - Desktop Support Tools - Province Owned

Software running on delivery staff desktops (including web-based apps) used to provide support or manage the Services

See Definition of Additional Notes codes at bottom of this sheet. This column on this one sheet identifies the expected duration of the EDS use of the software.

** If EDS decides to purchase the software **

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee	Relationship	Transferability
HP	HP Insight Manager S. 15 S. 15 HP Rapid Deployment Pack S. 15 Scripting Toolkit with Altiris Software S. 15 S. 15 HP OpenView Storage Builder and Storage Mirroring HP Service Centre and Connect-it S. 15 S. 15 HP SiteScope S. 15 S. 15 eXcursion S. 15 StorageWorks Command Console S. 15 S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	4 4 4 5 4	Province	N/A	Yes	Yes, this can be done on a one-time basis (allowing only one license transfer) depending on how long this stipulation must remain in effect and ensuring that the end-client is identified up front by EDS as part of the deal to ensure proper crediting.
Microsoft	Microsoft DFS - Distributed File System S. 15 S. 15 Microsoft Process Explorer S. 15 VISUALBASIC (VB) S. 15 S. 15 RDP – Remote Desktop Protocol from Microsoft S. 15 S. 15 ROBOCOPY S. 15 Microsoft Operations Manager (MOM) S. 15 S. 15 Microsoft.net framework S. 15 S. 15 Windows Resource Kit and Support Tools	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5 5 2 5 2 2 5 2 2 5	Province	N/A	Yes	I would assume yes as the licenses would be most probably purchased under the Customer agreement as EDS used as an Outsourcer.
Dartware, LLC	Dartware InterMapper S. 15 S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	4	Province	N/A	No	Yes. InterMapper is a perpetual license and when a reseller or service provider purchases on behalf of an end user, the license is issued in the end users (Company) name.
Oracle	ORACLE Client (for customers)	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	Yes	Yes

Remedy	Remedy agent	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	Yes	Yes, sold by BMC. if EDS has acquired additional Licenses for the Customer, those Licenses may be transferred to the Customer and enrolled in BMC's maintenance, enhancement and support plan upon payment of a transfer fee equal to 10% of the then current license fee. BMC and Customer shall enter into a new license agreement to govern such additional licenses.
Citrix	CITRIX Server and administrator consoles	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	Yes	Yes
Avocent	DSView3 S. 15 S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	4	Province	N/A	No	sent email; awaiting an answer
BC Government	BC Government DTS - Desktop Terminal Services – implementation of thin-client terminal server computing SFPApp* DiskScan* Queue Scan* Queue Creator* Enumerate Queues* Mailing List* All Shares Report* Protected Folder Creator* Role Group Report* Group Members* Group Memberships* IDIR User report* SFP Group Rename* Monthly Billing* Monthly Billing Exceptions (obsolete)* Server-Client Matrix* Daily Home Drive Report* Security Analyzer* Queue Management Automated Spreadsheet* FindQueue* SFP Print Queue Statistics* Ushare Split Assistant* Rename In Place* FormatRAW*	Province Proprietary Software	N/A	TBD	2 5 5 5 5 5 5 5 5 5 5 5 5 5 3 3 5 5 5 5 5 5 5 5 5	Province	N/A	No	No, not sure this is addressable
Eclipse	BIRT	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	No	Free software: http://www.eclipse.org/birt/phoenix/
MIT License (free software license)	PuTTY S. 15 S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	2	Province	N/A	No	Not applicable, this is a free software
Websense, Inc	S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	Yes	Yes, they prefer that the subscription be in the enduser name when we buy, but we can have you as a contact. We have worked with EDS before on projects and this has not been an issue.
Symantec	S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	1 5 5	Province	N/A	Yes	Yes

	S. 15	Province Licensed Software			5				
Check Point	Check Point S. 15 S. 15 Check Point S. 15 S. 15 Check Point S. 15 S. 15 Checkpoint S. 15 S. 15 Checkpont S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	4 4 4 4 4	Province	N/A	No	Yes
	Entrust S. 15	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A		
	ISM ActiveDirectoryUserInfoTool	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	2	Province	N/A		
Quest	Quest Toad DBA Suite for Oracle	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	Yes	Yes
BMC	Remedy Action Request System	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	5	Province	N/A	Yes	Yes, sold by BMC. if EDS has acquired additional Licenses for the Customer, those Licenses may be transferred to the Customer and enrolled in BMC's maintenance, enhancement and support plan upon payment of a transfer fee equal to 10% of the then current license fee. BMC and Customer shall enter into a new license agreement to govern such additional licenses.
VMware	VMware Converter Enterprise Client VMWare desktop - Allows creation of operating system images on Linux workstations. VMWare Infrastructure Client VMware Remote Console VMware Server VMware Virtual Infrastructure S. 15 VMware Workstation	Province Licensed Software	N/A	Not Applicable as S/W License remains under the Province's name.	3 3 3 3 3 3 5	Province	N/A	Yes	Yes, licenses need to be owned by EDS for a minimum of 12 months

* **BC Government SFP management scripts and utilities**

Additional Notes Legend

1-Software not required by EDS
2- Only required on Province PCS - approximately 3 to 4 months
3-Only required until EDS server management processes and tools implemented - month ?
4-Required until Transformation is complete
5-Long term use until tool evolution replaces product - impossible to accurately predict

Schedule H2 - Desktop Support Tools - EDS Owned

Software running on delivery staff desktops (including citrix and web-based apps) used to provide support or manage the Services

Third party	Software	Type of Software	Transfer Status (See Tab)	Assignable	Additional Notes	Responsible for S/W	Transfer Fee
EDS	Digital Workflow Web S. 15	SP Proprietary Software	No	No - EDS IP		EDS	N/A
Computer Associates	eHealth CA Unicenter S. 15 eTrust Policy Compliance Manager	SP Leveraged Software	No	No. The S/W is licensed under an annual term license and it's not transferable		EDS	N/A
Citrx	CITRIX Server and administrator consoles	SP Licensed Software	Yes	Yes, intention to transfer the S/W Licenses needs to be communicted to the publisher at the time of the acquisition of the Licenses		EDS	No Fee
EMC	EMC NAVIclient S. 15 NAS management tools Other SAN mgmt sofware	SP Licensed Software	Yes	Yes		EDS	No Fee
Brocade Communications Systems, Inc.	Brocade SAN Health S. 15 Brocade Fabric Manager S. 15	SP Licensed Software	To be notified	TBD		EDS	To be notified
PuTTY	PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator.	SP Licensed Software	Yes	Freeware		EDS	No Fee
VMware	VIM client (for VMWare access)	SP Licensed Software	Yes			EDS	No fee
Veritas	S. 15	SP Licensed Software	Yes			EDS	No Fee
Veritas		SP Licensed Software	Yes			EDS	No Fee
Winzip	Winzip	SP Licensed Software	Yes			EDS	No Fee
McAfee	McAfee Management Console	SP Leveraged Software	No	Not assignable as S/W is licensed under an annual term license. If a perpetual license was acquired, the S/W could be assigned back to the Province		EDS	N/A
Autopage	Autopage Client	SP Licensed Software	Yes			EDS	N/A