EXTENSION AND AMENDING AGREEMENT

This Extension and Amending Agreement (the **"Amending Agreement"**) is made to be effective the 1st day of June, 2022 (the "**Effective Date**")

BETWEEN:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, represented by the Minister Responsible for the BC Public Service Agency

(the "**Province**")

AND:

THE CANADA LIFE ASSURANCE COMPANY, an insurance company amalgamated under the laws of Canada and having a registered office at 100 Osborne Street North, Winnipeg, Manitoba R3C 1V3

(the "**Contractor**")

BACKGROUND:

A. The Province issued the Request for Proposals ON-003111 ("RFP") to procure Long Term Disability Plan Administration Services, and The Great-West Life Assurance Company was the successful proponent.

B. The Province entered into the LTD Plan Administration Services Agreement dated for reference June 1, 2018 (the "Original Agreement" or "Agreement") with The Great-West Life Assurance Company (the "Original Contractor").

C. On January 1, 2020, the Original Contractor, The Canada Life Assurance Company, London Life Insurance Company, Canada Life Financial Corporation and London Insurance Group Inc. were amalgamated under the laws of Canada and formed the Contractor.

D. Under the Agreement, the Province may, in its sole discretion, extend the term of the Agreement for one (1) additional two (2) year period and one (1) further additional one (1) year period.

E. The parties wish to confirm that the Province is deemed to have given notice, in accordance with the Agreement, to extend the Term of the Agreement for one two (2) year period, on the terms and conditions set out herein.

F. The parties also wish to further modify and amend the Agreement as set out herein.

IN CONSIDERATION OF these premises and other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged by each of the parties), the parties agree as follows:

LTD Plan Carrier

1. The parties acknowledge and agree that The Canada Life Assurance Company, as successor to the Original Contractor, is the LTD Plan Carrier under the Agreement.

Extension

2. The Term is hereby extended for the First Renewal Term (June 1, 2022 to May 31, 2024), on all of the same terms, conditions and covenants as are contained in the Original Agreement, except as modified and amended by this Amending Agreement.

Notices

3. The Agreement is amended by deleting the address and contact information in section 19.01(d) and replacing it with the following:

BC Public Service Agency
2nd Floor – 810 Blanshard Street
Victoria, BC V8W 2H2

Attention: Cindy Lew, Senior Manager, Corporate Health Programs
Email Address: Cindy.Lew@gov.bc.ca

The Canada Life Assurance Company
Suite 219 – 3531 Uptown Boulevard
Victoria, BC V8Z 0B9

Bryan Briere, Senior Account Executive
Email Address: bryan.briere@canadalife.com

Adjusted Fees

4. In accordance with section 3(a)(ii) of Schedule B, the parties agree that the 2022/20223 Monthly Fee during the first year of the First Renewal Term is $ $113,792 , which is apportioned as follows:

   i. Subject to paragraph 3.1 of Schedule B, $ 8,853 per month for providing the Subrogation and Overpayment Core Services, and

   ii. $ 104,939 per month for providing all other Core Services.

5. In accordance with section 3(b)(ii) of Schedule B, the parties agree that the 2022/2023 Hourly Fee during the first year of the First Renewal Term is $ 156 .

Schedules

6. The Agreement is amended by deleting Schedule "D" – Privacy Protection Schedule, and replacing it with Schedule "D" attached to this Amending Agreement.

7. The Agreement is amended by deleting Schedule "E" – Security Schedule and replacing it with Schedule "E" attached to this Amending Agreement.

8. The Agreement is amended by adding the following at the end of Article 22:

> "22.15 Any terms set out in the attached Schedule H apply to this Agreement."

and by adding the attached Schedule "H" – Tax Verification Schedule as Schedule "H" of the Agreement.

General

9. Unless the context otherwise requires, or unless otherwise defined in this Amending Agreement, any capitalized terms in this Amending Agreement will have the meanings given to them in the Agreement.

10. Time will remain of the essence of the Agreement, as modified and amended by this Amending Agreement.

11. The Agreement, as modified and amended by this Amending Agreement, is ratified and confirmed.

12. This Agreement will take effect on the Effective Date regardless of the date that it is executed by the parties.

13. This Amending Agreement may be entered into by a separate copy of this Amending Agreement being signed by, or on behalf of, each party, and that signed copy being delivered to the other party by a method agreed to by the parties (including by email in scanned PDF format), each of which will be deemed to be an original and all of which taken together will have the same effect as if each party had signed the same document.

IN WITNESS WHEREOF the parties have executed this Amending Agreement on the respective dates set out below.

SIGNED on the 1st day of June, 2022 by the Contractor (or, if not an individual, on its behalf by its authorized signatory):

Bryan Briere
Signature

Bryan Briere
Print Name

Sr. Account Executive
Print Title

SIGNED on the 2nd day of June, 2022 on behalf of the Province by its duly authorized representative:

Bobbi Sadler
Signature

Bobbi Sadler
Print Name

Deputy Minister
Print Title

Schedule "D" – Privacy Protection Schedule

Definitions

1. In this Schedule,

(a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* including any regulation made under it;

(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 Contractor as a result of the Agreement or any previous agreement between the Province and the Contractor dealing with the same subject matter as the Agreement;

(d) "**privacy course**" means the Province's online privacy and information sharing training course or another course approved by the Province; and

(e) "**public body**" means "public body" as defined in the Act;

(f) "**third party request for disclosure**" means a subpoena, warrant, order, demand or request from an authority inside or outside of Canada for the unauthorized disclosure of personal information to which the Act applies;

(g) "**service provider**" means a person retained under a contract to perform services for a public body; and

(h) "**unauthorized disclosure of personal information**" means disclosure of, production of or the provision of access to personal information to which the Act applies, if that disclosure, production or access is not authorized by the Act.

Purpose

2. The purpose of this Schedule is to:

(a) enable the Province to comply with the Province's statutory obligations under the Act with respect to personal information; and

(b) ensure that, as a service provider, the Contractor is aware of and complies with the Contractor's statutory obligations under the Act with respect to personal information.

Acknowledgements

3. The Contractor acknowledges and agrees that

(a) it is a service provider and, as such, the requirements and restrictions established by Part 3 of the Act apply to the Contractor in respect of personal information;

(b) unless the Agreement otherwise specifies, all personal information in the custody of the Contractor is and remains under the control of the Province; and

(c) unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect, use, disclose or store personal information that relates directly to and is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Collection of Personal Information

4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect or create personal information that relates directly to and is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

5. The Contractor must collect personal information directly from the individual the information is about unless:

   (a) the Province provides personal information to the Contractor;

   (b) the Agreement otherwise specifies; or

   (c) the Province otherwise directs in writing.

6. Where the Contractor collects personal information directly from the individual the information is about, the Contractor must tell that individual:

   (a) the purpose for collecting it;

   (b) the legal authority for collecting it; and

   (c) the name and contact information of the individual designated by the Province to answer questions about the Contractor's collection of personal information.

Privacy Training

7. The Contractor must ensure that each individual who will provide services under the Agreement that involve the access, collection or creation of personal information will complete, at the Contractor's expense, the privacy course prior to that individual providing those services.

8. The requirement in section 7 will only apply to individuals who have not previously completed the privacy course.

Accuracy of Personal Information

9. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Province to make a decision that directly affects the individual the information is about.

Requests for Access to Information

10. If the Contractor receives a request for access to information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Contractor to provide such access. If the Province

has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of Personal Information

11. Within 5 Business Days of receiving a written direction from the Province to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

12. When issuing a written direction under section 11, the Province must advise the Contractor of the date the correction request was received by the Province in order that the Contractor may comply with section 13.

13. Within 5 Business Days of correcting or annotating any personal information under section 11, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was received by the Province, the Contractor disclosed the information being corrected or annotated.

14. If the Contractor receives a request for correction of personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of Personal Information

15. Without limiting any other provision of the Agreement, the Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including without limitation by ensuring that the integrity of the personal information is preserved. Without limiting the general nature of the foregoing sentence, the Contractor will ensure that all personal information is securely segregated from any information under the control of the Contractor or third parties to prevent unintended mixing of personal information with other information or access to personal information by unauthorized persons and to enable personal information to be identified and separated from the information of the Contractor or third parties.

Storage of and Access to Personal Information

16. The Contractor must comply with the requirements under the Act concerning storage of personal information outside of Canada, including, if required by the Province, by supporting the Province with completion of such assessments as may be required by law.

17. The Contractor must not change the location where personal information is stored without receiving prior authorization of the Province in writing.

18. Without limiting any other provision of the Agreement, the Contractor will implement and maintain an access log documenting all access to personal information, including a list of all persons that access any personal information. The Contractor will provide a copy of the access log to the Province upon request.

Retention of Personal Information

19. Unless the Agreement otherwise specifies, the Contractor 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

20. Unless the Province otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement. For clarity, unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must not anonymize, aggregate or otherwise alter or modify personal information, including by converting personal information into non-personal information, or analyze personal information (whether by manual or automated means) for any purpose, including for the purpose of developing insights, conclusions or other information from personal information.

Metadata

21. Where the Contractor has or generates metadata as a result of services provided to the Province, where that metadata is personal information, the Contractor will:

(a) not use it or disclose it to any other party except where the Agreement otherwise specifies; and

(b) remove or destroy individual identifiers, if practicable.

Disclosure of Personal Information

22. Unless the Province otherwise directs in writing, the Contractor may only disclose personal information to any person other than the Province if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

23. If in relation to personal information, the Contractor:

(a) receives a third-party request for disclosure;

(b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a third-party request for disclosure; or

(c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a third-party request for disclosure,

subject to section 24, the Contractor must immediately notify the Province.

24. If the Contractor receives a third-party request described in section 23(a) or (b) but is unable to notify the Province as required by section 23, the Contractor must instead:

(a) use its best efforts to direct the party making the third-party request to the Province;

(b) provide the Province with reasonable assistance to contest the third-party request; and

(c) take reasonable steps to challenge the third party-request, including by presenting evidence with respect to:

(i) the control of personal information by the Province as a public body under the Act;

(ii) the application of the Act to the Contractor as a service provider to the Province;

(iii) the conflict between the Act and the third-party request; and

(iv) the potential for the Contractor to be liable for an offence under the Act as a result of complying with the third-party request.

Notice of Unauthorized Disclosure

25. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information, the Contractor must immediately notify the Province.

Compliance with the Act and Directions

26. The Contractor must in relation to personal information comply with:

(a) the requirements of the Act applicable to the Contractor as a service provider, including any regulation made under the Act and the terms of this Schedule; and

(b) any direction given by the Province under this Schedule.

27. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

28. The Contractor will provide the Province with such information as may be reasonably requested by the Province to assist the Province in confirming the Contractor’s compliance with this Schedule.

Notice of Non-Compliance

29. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply in any respect, with any provision in this Schedule, the Contractor 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

30. 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 Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

31. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

32. Any reference to “Contractor” in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with the requirements of the Act applicable to them.

33. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

34. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act, including any regulation made under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

35. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of the Agreement or the law of any jurisdiction outside Canada.

36. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

Schedule "E" – Security Schedule

Definitions

1. In this Schedule:

(a) "**Device**" means any device to manage, operate or provide the Services or to connect to any Systems or any Province system or network, or that is capable of storing any Protected Information, and includes any workstation or handheld device the Contractor authorizes Personnel to use in relation to this Agreement;

(b) "**Facilities**" means the physical locations (excluding those of the Province) the Contractor uses to provide the Services, or to house Systems or records containing Protected Information;

(c) "**Least Privilege**" means the principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks so as to limit the damage that can result from accident, error or unauthorized use;

(d) "**Need-to-Know**" means the principle where access is restricted to authorized individuals whose duties require such access and not merely because of status, rank or office;

(e) "**Personnel**" means all individuals hired or used by the Contractor and Subcontractors to perform the Contractor's obligations under this Agreement, including unpaid volunteers and the Contractor or a Subcontractor if an individual;

(f) "**Policies**" means the intentions and directions of an organization or part of it, as expressed in record form by its top management (including, for example, policies, directions, standards, practices, procedures and guidelines);

(g) "**Protected Information**" means any and all:

(i) "personal information" as defined in the Privacy Protection Schedule if attached;

(ii) information and records of information the Contractor is required to treat as confidential under this Agreement; and

(iii) records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked or instructed by the Province to be so preserved or otherwise treated as "Protected Information" under this Agreement;

(h) "**Security Event Logs**" means any logs (also known as audit records) of events, notifications or alerts that any component of any Device or other device (not limited to security device), or any Systems or other system or software is technically capable of producing in relation to its status, functions and activities that may be used for such purposes as security investigations, auditing, monitoring and determining security incidents (examples of components capable of producing such logs include firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, dynamic host configuration protocols, dynamic naming services, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application firewalls);

(i) “**Systems**” means any systems, subsystems, equipment, infrastructure, networks, management networks, servers, hardware and software the Contractor uses in relation to this Agreement, including for managing, operating or providing the Services, but excluding any the Province owns or makes available to the Contractor for the Contractor to use in relation to this Agreement;

(j) “**Tenancy**” means those components of the Systems that:

(i) directly access and store Protected Information,

(ii) relate to Protected Information or the Province’s tenancy activities, or

(iii) are customer facing and managed by the Province in its use of the Services; and

(k) “**Tenancy Security Event Logs**” means Security Event Logs that relate to Tenancy, including:

(i) log-on/log-off information about Province user activities, and

(ii) application logs, web server log, file server logs, database logs of applications, web servers, file servers or database servers or any other logs that directly store, access or contain Protected Information.

Additional obligations

2. The Contractor must comply with Appendix G1 if attached.

PERSONNEL

Confidentiality agreements

3. The Contractor must not permit any person the Contractor hires or uses to access or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under this Agreement.

Personnel security screening

4. The Contractor may only permit individual Personnel to have access to any Protected Information or other asset of the Province (including to any system, network or device the Province makes available to the Contractor) in relation to this Agreement, if, after:

(a) verifying their identity and relevant education, professional qualifications and employment history;

(b) completing a criminal record check that is updated at least every five years;

(c) requiring Personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law;

(d) performing any additional screening this Agreement or applicable law may require; and

(e) performing any additional background checks the Contractor considers appropriate,

the Contractor is satisfied that the individual does not constitute an unreasonable security risk.

5. If any criminal record check or proactive disclosure reveals a prior criminal offence or pending criminal matter, the Contractor must make a reasonable determination of whether the applicable person constitutes an unreasonable security risk, taking into consideration the duties of the individual and the type and sensitivity of information to which the individual may be exposed.

6. If the Contractor is an individual, the Province may subject the Contractor to the screening requirements in this Schedule.

Personnel information security training

7. Unless otherwise specified in this Agreement, the Contractor must ensure all Personnel complete any relevant information security training, at the Contractor's expense, before they provide any Services, or receive or are given access to any Protected Information or any system, device or secure facility of the Province, and thereafter at least annually.

Security contact

8. If not set out elsewhere in this Agreement, the Contractor (but not a Subcontractor) must provide in writing to the Province the contact information for the individual who will coordinate compliance by the Contractor and all Subcontractors and act as a direct contact for the Province on matters relating to this Schedule.

Supply chain

9. The Contractor must ensure that the security requirements of those in its upstream and downstream supply chain are documented, followed, reviewed, and updated on an ongoing basis as applicable to this Agreement.

GENERAL POLICIES AND PRACTICES

Information security policy

10. The Contractor must have an information security Policy that is:

(a) based on recognized industry standards; and

(b) reviewed and updated at least every three years.

Compliance and Standard for Security Controls

11. Unless this Agreement otherwise specifies, the Contractor must apply controls and security management practices to manage or operate Protected Information and Systems, Devices, and Facilities that are compliant with or equivalent to the following Province's Policies accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures:

(a) "Information Security Policy";

(b) government wide IM/IT Standards; and

(c) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.

Contractor security risk assessments

12. The Contractor must undertake a security threat and risk assessment against an industry security standard before placing any new or materially changed Systems or services into production.

Change control and management

13. The Contractor must:

(a) implement and maintain change control processes for Facilities, Systems and Devices in line with applicable security best practices to reduce security-related risks with respect to implemented significant changes; and

(b) ensure that adequate testing of any change is completed before the change is put into production.

Backups and restores

14. The Contractor must ensure that:

(a) it has a backup Policy that is followed and is reviewed, updated and tested at least annually;

(b) backups are taken and tested in accordance with the Contractor's backup Policy, but in any event at least annually; and

(c) frequency and completeness of backups is based on reasonable industry practice.

Business continuity plan and disaster recovery plan

15. The Contractor must ensure that it has a documented business continuity plan and a disaster recovery plan that is reviewed at least annually.

16. The Contractor must ensure that Facilities and Systems are protected from loss, damage or other occurrence, including fire and environmental hazards and power interruptions, that may result in any of those Facilities and Systems being unavailable when required to provide the Services.

Security Incident Response and Management

17. The Contractor must ensure that it has a security incident management Policy and response plan that is reviewed at least annually.

PROTECTED INFORMATION AND DATA SECURITY

Encryption

18. The Contractor must ensure that:

    (a) encryption of data at rest is implemented and is maintained in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, for all Protected Information stored on Systems and Devices; and

    (b) encryption end-to-end is implemented for all Protected Information in transit.

No storage on unencrypted portable media

19. The Contractor must ensure that no Protected Information is stored on portable media for transport outside of the Facilities or Systems without both the prior written approval of the Province and ensuring that the portable media and the Protected Information are encrypted.

Encryption standard

20. For sections 18 and 19, encryption must comply with the Province's "Cryptographic Standards for Information Protection" accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures.

Isolation controls and logical isolation of data

21. The Contractor must implement and maintain the logical isolation of Protected Information, in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure.

ACCESS AND AUTHENTICATION

User Identifiers

22. The Contractor must assign and ensure that user identifiers are unique and personal for log in to Systems and Devices.

Access

23. The Contractor must implement, follow, and regularly review and update, access control Policies that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts for Facilities, Systems and Devices within the Contractor's control.

24. The Contactor must ensure that all access to Protected Information and to Facilities, Systems and Devices is based Least Privilege and Need-to-Know" based on role and responsibilities. The Contractor must identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse.

25. The Contractor must verify an individual's identity before assigning the individual a unique identifier that would give them access to Facilities, Systems or Devices.

26. The Contractor must implement a formal user registration process for Personnel that includes:

    (a) verification of access levels;

    (b) creating and maintaining records of access privileges;

    (c) audit processes; and

    (d) actions to ensure access is not given before approval is granted by the Contractor.

27. The Contractor must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts.

28. The Contractor must implement a monitoring process to oversee, manage and review Personnel access rights and roles at regular intervals.

29. The Contractor must ensure that all Systems and Devices:

    (a) are configured in alignment with industry standards;

    (b) enforce a limit of consecutive invalid logon attempts by a user during a predetermined time period;

(c) automatically lock the applicable account and Systems after failed logon failures;

(d) limit the number of concurrent sessions;

(e) prevent further access to Systems by initiating a session lock; and

(f) provide the capability of disconnecting or disabling remote access to the Systems.

Authentication

30. The Contractor must use or require complex passwords or personal identification numbers (PINs) that are not shared, default or blank and that are encrypted (not displayed) when entered, biometric accesses, keys, smart cards, other logical or access controls, or combinations of them, to control access to Protected Information and to Systems and Devices.

31. The Contractor must ensure that Systems for password-based authentication:

(a) enforce minimum password complexity, including requiring passwords to be case sensitive, contain a minimum of eight characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters;

(b) change authentication passwords regularly at predetermined intervals, but at a minimum semi-annually;

(c) store and transmit only encrypted representations of passwords;

(d) enforce password minimum and maximum lifetime restrictions;

(e) prohibit password reuse;

(f) prevent reuse of identifiers; and

(g) disable the identifier after ninety days of inactivity.

Highly sensitive Protected Information

32. If this Agreement or the Province under this Agreement indicates that any Protected Information is highly sensitive, the Contractor must also ensure that Systems enforce with respect to that Protected Information:

(a) two-factor authentication for access;

(b) enhanced logging that logs all accesses;

(c) request based access; and

(d) no standing access rights.

SECURITY EVENT LOGS

Log generation, log retention and monitoring

33. The Contractor must ensure that logging of Security Event Logs is enabled on all applicable Systems components

34. The Contractor must retain Security Event Logs for the Systems online for a minimum of 90 days and either online or off-line for an additional period of time adequate to enable the Contractor to conduct effective security investigations into suspected or actual security incidents.

35. The Contractor must retain Tenancy Security Event Logs online for a minimum of 90 days and either:
(a) such additional period of time as the Province may instruct; or
(b) ensure that the Tenancy offers the technical capability for the Province to retain the Tenancy Security Event Logs,

to enable the Province to comply with an information schedule approved under the *Information Management Act* or other retention period required by law.

36. Upon the Province's request, the Contractor must ensure that the Tenancy offers the technical capability for the Province to enable or configure the forwarding, extraction, backup of Tenancy Security Event Logs from the Tenancy to the Province's security information and event management system or to an external log storage and retention system.

37. The Contractor must review Security Event Logs regularly to detect potential security incidents, using automated tools or equivalent processes for the monitoring, review, correlating and alerting of Security Event Logs.

PROVINCE PROPERTY

Access to Province facilities, systems or networks

38. If the Province makes available any facilities, systems, networks or devices for use of the Contractor in relation to this Agreement, the Contractor must comply with, and permit access on its behalf only by those authorized Personnel who have been instructed to comply with, the Province's Policies then applicable to their acceptable use, access and protection accessible at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures, including:

(a) "Appropriate Use Policy" (as also referenced in chapter 12 of the Province's "Core Policy and Procedures Manual");

(b) "Information Security Policy";

(c) government wide IM/IT Standards; and

(d) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.

39. The Province has the rights to:

(a) not make any particular Province facility, system, network or device available before the Contractor or individual Personnel or both agree to a form of agreement acceptable to the Province on acceptable use, protection of, and access to, such facility, system, network or device, or at all;

(b) not permit connection to any particular Province system or network until satisfied with the controls applied and the security status of the Device to be connected;

(c) keep facilities access logs and Security Event Logs, and to otherwise monitor and analyze use of Province facilities, systems and networks to verify compliance, investigate suspected or actual breaches or information incidents and protect the Province's assets, including records, in compliance with applicable laws, including the *Freedom of Information and Protection of Privacy Act* and *Information Management Act*, and the Province's Policies; and

(d) limit or revoke access to any Province systems, facility or device at its discretion.

Application development

40. If the Services include software development, the Contractor must ensure that the applications and programming interfaces are developed according to industry standards and Province's Policies applicable to application development standards. The Contractor must use secure application development practices for the development of the software.

FACILITIES, SYSTEMS, DATABASE AND DEVICE SECURITY

Physical security

41. The Contractor must ensure that adequate physical controls and processes are implemented to ensure that only authorized persons have physical access to the Facilities and Systems.

42. The Contractor must develop, document, and disseminate a physical and environmental protection Policy that it reviews at least annually.

43. The Contractor must review physical access logs at least once monthly.

44. The Contractor must ensure that physical security of any Systems or Facilities being used or capable of being used to house Protected Information meets a standard as would be reasonably expected to provide adequate protection based on the value of the data being protected and the environment in which the Systems or Facilities are located. At a minimum, this should include:

(a) hardening of the perimeter of the Facilities;

(b) physical separation of public and restricted spaces;

(c) Intrusion Alarm System (IAS) partitioned to ensure areas containing Protected Information are protected at all times;

(d) Access Control Systems (ACS) and/or Key Management processes; and

(e) visitor and identity management processes – including access logs and identification badges.

Separation of production from test environments

45. The Contractor must not use any production data in any development, test or training environments used for the Services without the Province's prior written consent. If the Province gives such consent, the production data must, at minimum, be obfuscated (for example, by using data masking functionality).

46. The Contractor must keep its development, test and training environments separate from its production environments used for the Services at all times, even in case of failure.

Systems (including servers) hardening

47. The Contractor must:

(a) harden all Systems against attack and misuse, using appropriate security best practices for the hardening of the specific deployed platform, before placing those Systems into production;

(b) ensure that all unsecured and unneeded ports, services, applications, protocols and network communicating applications are uninstalled or disabled on all Systems;

(c) applying Least Privilege, ensure that the Contractor only configures and makes operational ports, services, applications, protocols and network communicating applications based on the functional requirements of the respective Systems;

(d) ensure that default passwords and shared accounts are not used for any Systems; and

(e) in relation to Systems, implement server hardening using configuration security best practices (for example, Center for Internet Security, Inc. (CIS) Benchmarks or equivalent) for any server operating systems, server virtualization, server middleware (for example, web servers and database servers) and application servers.

Perimeter controls (firewall and intrusion prevention system) and network security

48. The Contractor must:

(a) implement stateful packet inspection firewalls to control traffic flow to and from Systems and Tenancy at all times, and configure the stateful packet inspection firewalls applying security best practices and Least Privilege;

(b) implement an intrusion prevention System to control and filter traffic flow leaving and entering Systems and Tenancy at all times, and configure the intrusion prevention System applying security best practices; and

(c) implement a secure network perimeter and network segmentation for Systems, with ingress and egress points that are known and controlled.

Application firewall

49. The Contractor must implement application layer firewalls on Systems:

(a) at such level of protection as the Province may instruct ; and

(b) to detect and mitigate application attacks (for example, brute force, OWASP Top 10, SQL injection, cross site scripting).

Management network

50. The Contractor must ensure that for any Systems:

(a) the management network remains logically separated from any other zone and is not directly accessible from the Internet;

(b) the management network is internally segmented, with each server's dedicated network interface on its own segmented network and that interfaces on the management network do not have visibility to each other; and

(c) all access to the management network is strictly controlled and exclusively enforced though a secure access gateway, bastion host or equivalent.

Remote management and secure access gateway

51. The Contractor must perform any remote management of Systems or Devices in a secure manner, using encrypted communication channels and adequate access controls.

Database security

52. The Contractor must ensure that for any Systems:

(a) database maintenance utilities that bypass controls are restricted and monitored;

(b) there is a formal approval process in place for handling requests for disclosure of database contents or for database access, including steps to evaluate privacy impacts and security risks of such requests; and

(c) methods to check and maintain the integrity of the data are implemented (for example, consistency checks and checksums).

53. For database security, the Contractor must implement logical isolation and encryption of Protected Information.

Device security and antivirus scanning

54. The Contractor must ensure all Devices:

(a) have antivirus and malware protection as appropriate for the particular Device active at all times;

(b) are configured to perform antivirus scans at least once per week;

(c) have host based firewall configured, enabled and active at all times; and

(d) have all patches and appropriate security updates installed for the operating system and all installed software.

VULNERABILITY PREVENTION, SCANNING AND MANAGEMENT

Proactive management

55. The Contractor must:

(a) obtain information in a timely basis about technical vulnerabilities relating to Systems and Devices; and

(b) implement processes to stay current with security threats.

Patching

56. The Contractor must patch all Systems regularly in line with security best practices and ensure that current software, operating systems and application patching levels are maintained.

57. The Contractor must ensure that all Systems have all patches installed on a regular schedule, within the time frame recommended by the manufacturer unless the Province otherwise consents in writing.

58. The Contractor must ensure that vulnerabilities are remedied and patches installed on an accelerated basis for zero-day, critical and high vulnerabilities. For zero-day vulnerabilities, the Contractor must implement appropriate mitigation measures promptly on notification of the zero-

day vulnerability. The Contractor must remediate zero-day, high and critical vulnerabilities through patching, decommission, or compensating controls.

59. The Contractor must patch high vulnerabilities within 30 days or less of discovery and patch medium vulnerabilities within 90 days or less of discovery.

Vulnerability Scanning

60. The Contractor must ensure that a vulnerability scan is completed on components of all Systems:

    (a) with any identified vulnerabilities remedied, before being placed into production; and

    (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Web application vulnerability scanning

61. The Contractor must ensure that a vulnerability scan is completed on any web applications used for Tenancy or in any other Systems:

    (a) and on any major changes to such web applications, with any identified vulnerabilities remedied, before being placed into production; and

    (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Antivirus and malware scanning

62. The Contractor must ensure that all Systems servers:

    (a) have antivirus and malware protection configured, active and enabled at all times;

    (b) have antivirus and malware definitions updated at least once a day; and

    (c) are configured to undergo a full anti-virus scan for latent infections (to detect infections missed by the real-time agent) at least once a week.

DISPOSALS

Asset disposal

63. The Contractor must ensure that all disposals of assets used in providing or relating to the Services are done in a secure manner that ensures that Protected Information cannot be recovered.

Asset management

64. The Contractor must have asset management and disposal Policies that are followed, and reviewed and updated regularly in line with security best practices, and that address hardware, software and other critical business assets.

65. The Contractor must keep an asset management inventory that includes the name of the System, location, purpose, owner, and criticality, with assets added to inventory on commission and removed on decommission.

Information destruction and disposal

66. Unless this Agreement otherwise specifies, the Contractor must retain all records containing Protected Information in the Contractor's possession until instructed by the Province in writing to dispose or deliver them as instructed.

67. The Contractor must securely erase:

    (a) records that contain Protected Information and Tenancy Security Event Logs when instructed in writing by the Province; and

    (b) any backup, transitory and extra copies of records that contain Protected Information or Tenancy Security Event Logs when no longer needed in relation to this Agreement.

68. The Contractor must ensure that Protected Information and Tenancy Security Event Logs on magnetic media are securely wiped by overwriting using procedures and adequate media wiping solutions, degaussing, or other method in line with security best practices for disposal of media.

NOTICES, INCIDENTS AND INVESTIGATIONS

Notice of demands for disclosure

69. In addition to any obligation the Contractor may have to notify or assist the Province under applicable law or this Agreement, including the Privacy Protection Schedule if attached, if the Contractor is required (including under an enactment or a subpoena, warrant, order, demand or other request from a court, government agency or other legal authority) to produce, provide access to or otherwise disclose any Protected Information, the Contractor must, unless prohibited by applicable law, immediately notify and provide reasonable assistance to the Province so the Province may seek a protective order or other remedy to prevent or limit the disclosure.

E-discovery and legal holds

70. The Contractor must fully co-operate with the Province to enable the Province to comply with e-discovery and legal hold obligations.

Incidents

71. In addition to any obligation the Contractor may have under applicable law, including the *Freedom of Information and Protection of Privacy Act,* or this Agreement, if, during or after the Term, the Contractor discovers a suspected or actual unwanted or unexpected event or series of events that threaten the privacy or security of Protected Information (including its unauthorized access, collection, use, disclosure, alteration, storage or disposal) or Tenancy, whether accidental or deliberate, the Contractor must:

    (a) immediately report the particulars of such incident to, and follow the instructions of, the Province, confirming any oral report with a notice in writing to the Province as soon as reasonably practicable (if unable to contact the Province's contract manager or other designated contact for this Agreement, the Contractor must follow the procedure for reporting and managing information incidents on the Province's website at https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents; and

    (b) make every reasonable effort to recover the records containing Protected Information and contain and remediate such incident, following such reasonable instructions as the Province may give.

Investigations support and security investigations

72. The Contractor must:

    (a) conduct security investigations in the case of incidents (including any security breach or compromise) affecting Devices, Facilities, Systems, Tenancy or Protected Information, collecting evidence, undertaking forensic activities and taking such other actions as needed;

    (b) provide the Province with any related investigation reports, which the Contractor may sanitize first;

    (c) upon the Province's request, provide the Province with any logs relating to such investigation reports as validation/confirmation of such investigation, which the Contractor may sanitize first; and

    (d) maintain a chain of custody in all such security investigations it undertakes.

73. Upon the Province's request, the Contractor must:

    (a) provide investigative support to the Province to enable the Province to conduct its own security investigations into incidents (including security breaches or compromises) affecting the Tenancy or Protected Information;

    (b) provide the Province with timely access via an on-line, real-time GUI (Graphic User Interface) facility to any Tenancy Security Event Logs and to other Security Event Logs for Systems (the latter of which the Contractor may sanitize first to mask or remove, for example, data pertaining to the Contractor's customers) to assist the Province in conducting the Province's security investigations, or in case of technical limitations, other method acceptable to the Province (for example, on-site visits to enable direct access to those Security Event Logs).

74. The Contractor must work with and support the Province if the Province needs assistance in legal proceedings in relation to security investigations related to Protected Information or Tenancy.

Province Security Threat and Risk Assessment ("STRA") support

75. The Contractor must, via its technical and security resources, support the Province in completing a STRA for the Services and to otherwise assess the risks associated with the Services, including by providing all information and documentation (for example, architecture diagrams, service architecture, controls architecture and technical information), which the Contractor may sanitize first and that the Province may reasonably require for such purpose.

Notification of changes

76. The Contractor must notify the Province of any changes to its security Policies, management practices and security controls described in this Agreement that may potentially negatively impact the security of Tenancy, Protected Information, or those Systems providing the Services.

Compliance verification

77. Upon the Province's request, the Contractor must provide, at no additional cost, the following security reports to the Province at least every six months during the Term:
    (a) vulnerability scan reports of those Systems providing the Services; and
    (b) patch status reports for those Systems providing the Services.

78. In addition to any other rights of inspection the Province may have under this Agreement or under statute, the Province has the rights, at any reasonable time and on reasonable notice to the Contractor, to:

    (a) request the Contractor to verify compliance with this Schedule and to keep security controls documentation or records to support compliance; and
    (b) enter on the Contractor premises and Facilities to inspect and to validate the Contractor's compliance with the security obligations under this Agreement

79. The Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section. If any non-compliance or deficiency is found, the Province may (in addition to any other rights it may have) require the Contractor, at the Contractor's expense, to develop and implement a corrective action plan within a reasonable time.

Notice of non-compliance

80. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor 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.

MISCELLANEOUS

Interpretation

81. In this Schedule, unless otherwise specified, references to sections by number are to sections of this Schedule.

82. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under this Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

83. Any reference to a specified Policy refers to it as may be revised or replaced from time to time.

84. If a provision of this Schedule conflicts with a documented process required by this Schedule to be created or maintained by the Contractor, the provision of the Schedule will prevail to the extent of the conflict.

Referenced documents

85. Policies and other documents of the Province referenced in this Schedule may be updated or replaced by the Province from time to time without notice, and if not found at the hyperlink or URL provided or via the Province's main website at http://www.gov.bc.ca, be obtained from the Province's contact for this Agreement.

Survival

86. Sections 63, 66, 67, 68, 69, 70, and 71 and other obligations of the Contractor in this Schedule which, by their terms or nature, are intended to survive the completion of the Services or the termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedule “H” – Tax Verification Schedule

1. In this Schedule:

   a) “**Tax Verification Letter**” means a letter issued by the Province of British Columbia’s Ministry of Finance verifying that the Contractor meets its applicable B.C. corporate income tax filing obligations and provincial sales tax (PST) filing and payment obligations; and

   b) “**Valid”** means that the Tax Verification Letter’s period of validity, as indicated on the Tax Verification Letter, has not ended.

2. As a condition of entering into this Agreement, the Contractor provided to the Province a Valid Tax Verification Letter.

3. Upon request by the Province, the Contractor must provide the Province with a new Valid Tax Verification Letter. Notwithstanding any other provision of this Agreement, the Contractor acknowledges and agrees that any extension or renewal of this Agreement is conditional upon the Province having, or receiving from the Contractor in response to a request from the Province, a Valid Tax Verification Letter prior to any such extension or renewal.