Office of the Chief Information Officer Policy Directive

DIRECTIVE:	1/14
SUBJECT:	Appropriate Use of Government Information and Information Technology Resources ("Appropriate Use Policy")
AUTHORITY:	Chapter 12 of the Core Policy and Procedures Manual (CPPM)
EFFECTIVE DATE	March 21, 2014

Purpose:

The purpose of this directive is to set out the policy requirements that all government employees must follow when:

- accessing and managing government information (particularly confidential information); and,
- using information technology (IT) resources.

Additional policies and procedures may be established at the ministry level to support employee compliance with, and monitoring of, this directive and/or to augment this directive with policies and procedures specific to that ministry's information holdings or organizational structure.

Compliance with this directive, and supporting ministry policies and procedures, will ensure that government information is appropriately protected while remaining accessible to those who need it and are authorized to access it. Ultimately, appropriate use of government information and IT resources will ensure that government is able to deliver effective and efficient services to citizens while meeting its statutory obligations to protect information.

Application:

This policy applies to all ministries, agencies, boards and commissions reporting or responsible to the Government of British Columbia.

Advice on this Directive:

Advice on this Directive can be obtained from the:

Strategic Planning and Policy Branch
Office of the Chief Information Officer
Ministry of Technology, Innovation and Citizens' Services

Email: CIOWebCommunications@gov.bc.ca

Version	Date	Changed By	Description of Change
1.0	March 21, 2014	Colleen Rice	
1.1	August 25, 2014	Colleen Rice	Update broken links
1.2	April 21, 2015	Colleen Rice	Update broken links
1.3	September 21, 2015	Colleen Rice	Update broken links
1.4	August 2, 2016	Sherri Kain	Update broken links and contact information

Table of Contents

Definitions:

The following key terms are defined below and appear in bold font throughout the document.

Confidential Information is a category of **Government Information** with confidentiality requirements. It includes, but is not limited to:

- cabinet confidences (for example, a briefing note to Cabinet);
- government economic or financial information (for example, information about a proposed administrative plan that has not yet been implemented or made public);
- information harmful to intergovernmental relations (for example, information received in confidence from another government);
- third party business information, where its disclosure could harm the third party;
- **Personal Information**;
- legal advice or law enforcement information.

Device: an **IT Resource** that can connect (wired, wireless or cellular) to the government network, including but not limited to computers, laptops, tablets, smartphones, and cellphones.

Employee: an individual working for the Government of British Columbia, including **Service Providers** or volunteers.

Government Information: means all recorded information relating to government business, regardless of format, that is received, created, deposited or held by any ministry, agency, board or commission reporting or responsible to the Government of British Columbia.

Information Incident is a single or a series of unwanted or unexpected events that threaten privacy or information security, including a privacy breach or the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information.

IT Resources: information and communication technologies that include, but are not limited to: information systems, **Devices,** and the government electronic network.

Least Privilege: a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Need-to-know: a principle where access is restricted to authorized **Employees** that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

Personal Information: is recorded information about an identifiable individual other than (business) contact information.

Portable Storage Device: is a portable (or removable) device that is primarily designed to store electronic information, for example an external hard drive or a USB flash drive.

Protected Government System: a computer system in a data centre that has met the approved security requirements for the storage of **Confidential Information** (for example, an **Employee's** network drives). This does not include the hard drives of computers, laptops, tablets, smartphones or other **Devices.**

Record: is anything that is recorded or stored by graphic, electronic, mechanical or other means, including books, documents, maps, drawings, photographs, letters, vouchers, and papers.

Service Provider: means a person retained under contract to perform services for the Government of British Columbia**.**

Roles and Responsibilities:

Deputy Ministers or Equivalent

Deputy Ministers (or equivalent positions) are responsible for ensuring that ministry specific policy and procedures are developed, where necessary, to support the Appropriate Use Policy.

Government Chief Information Officer

The Government Chief Information Officer is responsible for issuing corporate policy, directives and guidelines on the appropriate use of government **IT Resources** and **Government Information.**

Ministry Chief Information Officers or Equivalent

Ministry Chief Information Officers (or equivalent positions) are responsible for developing ministry-specific policies and procedures, where necessary, to support the Appropriate Use Policy.

In addition, Ministry Chief Information Officers are responsible for providing support to supervisors in their respective ministries to ensure that supervisors have the information and training necessary to fulfill their responsibilities as set out in this policy.

Supervisors

Supervisors are responsible for ensuring that **Employees** are made aware of their responsibilities concerning the appropriate use of **Government Information** and government **IT Resources**.

They are also responsible for ensuring that **Employee** access to **Confidential Information** is based on the principles of **Need-to-Know** and **Least Privilege** and for reviewing that access level annually.

They are responsible for ensuring that **Employees** receive the level of training (including privacy, security and records management training) necessary to perform their duties.

In addition, supervisors are responsible for approving the downloading of applications and software by **Employees**. This includes exercising due diligence to ensure that applications and software that are approved for download meet the requirements of this policy.

Further, supervisors are responsible for approving **Employees'** ability to work outside the workplace with **Confidential Information** and ensuring compliance with the Working Outside the Workplace Policy.

Employees

Employees are responsible for complying with this policy and for seeking direction from their supervisors if they have questions regarding this policy.

Policy:

A. General Requirements

1. **Employees** must comply with the Standards of Conduct for Public Service Employees when:

   a) collecting, accessing, using, disclosing or disposing of **Government Information**;
   b) using **IT Resources**, whether that use is directly related to their employment duties or not; and,
   c) accessing third party hosted sites (e.g. Facebook and Twitter) in a manner that could be perceived as representing government. For more information on the use of Social Media, please see the Social Media Guidelines.

2. Supervisors must ensure that **Employees** are made aware of their responsibilities concerning the appropriate management of **Government Information** and **IT Resources**:

   a) at the commencement of their employment;
   b) when a significant change occurs respecting their access to, or authorized use of, **Government Information** or their use of **IT Resources**, including but not limited to:
      i. the issuance a new **Device**; and
      ii. access to a new information database.
   c) when a new or updated version of this directive or similar policy is issued; and
   d) annually for **Employees** that have access to a significant amount of **Confidential Information**.

3. Supervisors must ensure that **Employees:**

   a) understand what **Confidential Information** is and the ministry policies and procedures that must be followed when accessing and managing **Confidential Information**; and
   b) have received training appropriate to their position respecting the management of **Confidential Information** (including privacy, security and records management training) and what to do if an **Information Incident** occurs.

   For further information on **Information Incidents** please refer to The Information Incident Management Process.

4. Ministry Chief Information Officers (or equivalent positions) must develop ministry-specific policies and procedures, where necessary, to support **Employee** compliance with, and monitoring of, this policy.

5. Deputy Ministers (or equivalent positions) must ensure that ministry-specific policies and procedures are developed, where necessary, to support **Employee** compliance with, and monitoring of, this policy.

B. Collection, Access, Use, Disclosure, Storage and Disposal of Government Information

6. **Employees** must collect, access, use, disclose and dispose of **Government Information** in accordance with policy and law. For example, disposal of information must be done in accordance with approved records schedules, and collection, access, use and disclosure of **Personal Information** must be in accordance with the *Freedom of Information and Protection of Privacy Act* and its supporting policies.

7. Supervisors must authorize an **Employee's** access to **Government Information** based on the principles of "**Need-to-know**" and "**Least Privilege**". Specifically, an **Employee** should have access to the least amount of **Confidential Information** that is necessary to perform their duties.

8. Supervisors must review an **Employee's** level of access to **Confidential Information** at least once per year to ensure that their access level remains necessary and appropriate for the performance of their duties.

9. **Employees** must not collect, access, use, disclose or dispose of **Confidential Information** unless authorized to do so and it is necessary for the performance of their duties.

10. **Employees** must respect intellectual property rights. For example, **Employees** must not use, reproduce, modify or distribute programs or data if they have not received permission from the intellectual property owner to do so.

For more information on intellectual property rights please contact the Intellectual Property Program.

11. **Employees** must store electronic **Records** that relate to government business in **Protected Government Systems**.

    a) In extenuating circumstances, an electronic government **Record** may be temporarily stored outside of a **Protected Government System**, as long as the following conditions are met:

        i. the electronic **Record** is stored on the system or **Device** only as long as is necessary to deal with the extenuating circumstance;
        ii. at the first available opportunity, the **Record** is transferred to a **Protected Government System**; and
        iii. duplicate copies of any electronic **Record** containing **Confidential Information** are deleted from the other system or **Device** as soon as possible.

b) The requirements set out in subsection (a) do not apply to an email **Record** that is automatically stored by government's email system on an **Employee's Device.**

12. **Employees** are responsible for ensuring that the **Confidential Information** they are working with is protected. This includes, but is not limited to:

    a) storing **Confidential Information** in **Protected Government Systems**, as set out in section 11, above;
    b) physically securing **Confidential Information** in their workspace (e.g. locked drawers or cabinets);
    c) only disclosing **Confidential Information** to authorized individuals in a secure manner according to ministry approved processes (e.g. **Portable Storage Devices** should only be used in extenuating circumstances when more secure methods are not available and must be encrypted); and
    d) limiting the amount of **Confidential Information**, particularly **Personal Information** (which is subject to legal restrictions), that is disclosed through email.

For further information on encryption standards, please see the Cryptographic Standards for Information Protection.

13. **Employees** may work outside the workplace with **Confidential Information** provided that they have their supervisor's approval and comply with all the provisions of this directive. In addition**, Employees** must:

    a) protect the information, particularly when working in a public environment (for example, ensuring that information is not viewable or accessible by others);
    b) limit the amount of printed materials that are used outside of the workplace (government **Devices** are more secure because they are protected with government security features); and
    c) follow the Working Outside the Workplace Policy.

14 If an **Information Incident** occurs, **Employees** and supervisors must follow the Information Incident Management Process which requires the immediate reporting of any suspected or actual **Information Incident** (including a privacy breach) to the Office of the Government Chief Information Officer and to the Ministry Chief Information Officer.

C. Use and Disposal of Government IT Resources

15. Reasonable personal use of government **IT Resources** by **Employees** is permitted. Personal use is reasonable provided that it:

    a) is limited during core business hours and does not interfere with the **Employee's** duties and responsibilities;
    b) is lawful;
    c) does not compromise the security of government **IT Resources** or **Government Information**; and
    d) is not used for personal financial gain.

16. For privacy reasons and to reduce the cost of electronic storage for government, **Employees** must limit the amount of personal **Records** they store on government systems.

17. **Employees** must use their government email accounts when conducting government business. This includes while working outside of the workplace.

    In extenuating circumstances, **Employees** may use their personal email or other non-government email, as long as the following conditions are met:

    a) a copy of the email is sent to their government email account, ensuring that the **Government Information** is stored in a **Protected Government System**;
    b) the email is immediately deleted from their personal or non-government email account as soon as possible after dealing with the extenuating circumstance; and
    c) the amount of **Confidential Information** collected, accessed, used or disclosed is limited to the least amount necessary to deal with the extenuating circumstance.

    For information on how to access government email accounts from a remote location, please see the Outlook Web App Guide.

18. **Employees** must not divulge, share or compromise their own or another **Employee's** government authentication credentials (e.g., passwords, access cards, etc.). This includes not divulging passwords to technical support.

19. **Employees** must report any lost or stolen **Device** or access card in accordance with Chapter 20 – Loss Management of the Core Policies and Procedures Manual (CPPM) and Procedure L – Loss Reporting of the CPPM.

20. **Employees** must follow the appropriate policies and procedures when disposing of **IT Resources**. For further information, please see the IT Asset Disposition Site.

D. Access to and Use of Applications and Software

21. **Employees** must have their supervisor's permission, and follow the established procedures, to download or use applications or software from the iStore or the Self-Serve Centre.

22. If an **Employee** wishes to download or use applications or software for government business purposes that are available through the iStore or the Self-Serve Centre and are also available from another source, the **Employee** must download or access the application or software from the iStore or the Self-Serve Centre.

23. **Employees** must not download or use applications or software for government business that are not available from the iStore or the Self-Serve Centre without the permission of their supervisor.

    Applications and software that are not available from the iStore or the Self-Serve Centre may present privacy or security concerns or could impose terms and conditions, such as indemnification clauses, that are unacceptable to government.

24. Supervisors must not permit an **Employee** to download or use applications or software that:

    a) are prohibited by the Government Chief Information Officer;
    b) present unacceptable privacy or security concerns; or
    c) impose unacceptable terms and conditions.

    With respect to section 2(c), supervisors should review their procurement responsibilities in the Core Policy and Procedures Manual - Chapter 6 Procurement before approving an application for download.

E. Monitoring and Investigations

25. Any collection, access, use, transmission, or disposal of **Government Information** or use of government **IT Resources**, whether for personal reasons or not, may be audited, inspected, monitored and/or investigated to:

    a) maintain, repair and manage **IT Resources** for the efficient operation of business systems;
    b) meet legal requirements to produce information, including by engaging in e-discovery;
    c) ensure accessibility of government **IT Resources** for the continuity of work processes;
    d) improve business processes and manage productivity; and
    e) ensure compliance with legislative and policy requirements, including the Standards of Conduct.

26. Allegations of inappropriate access, collection, use, disclosure, or disposal of **Government Information** or inappropriate use of government **IT Resources** will be investigated on a case-by-case basis. Investigations may include, but are not limited to, the search and/or seizure of **IT Resources**.

27. **Employees** who inappropriately access, collect, use, disclose or dispose of **Government Information** or inappropriately use **IT Resources** may be subject to disciplinary action, including dismissal, cancellation of contract, and/or other legal remedies.

Print and Close Cancel

Information Management and Information Technology Management

Information Management and Information Technology Management

Table of Contents

12.1 Objectives

The objectives of this chapter are to:

- Provide guidance for key legislation, including
  - *Document Disposal Act;*
  - *Electronic Transactions Act;*
  - *Freedom of Information and Protection of Privacy Act; and*
  - *Personal Information Protection Act*.
- Define authorities, responsibilities and accountabilities for information and technology management.
- Provide a policy framework within which government can derive the maximum benefits from the use of information and technology.
- Establish policies for the management of information and technology activities.

12.2 General

12.2.1 Principles

Information management is a core component of government infrastructure; it is the intellectual capital of responsible governance. Best practice policies and standards result in efficient, accountable and cost-effective use of resources. Information technology constitutes the full spectrum of technologies and services that support information management. The Government Chief Information Officer (CIO) is responsible for the corporate management of information and information technology. The principles underlying effective management are:

- information is a vital government asset that must be managed and, where appropriate, shared to maximize investments;
- information and technology are key components in delivering cost-effective government services to the public;

- information and technology have the potential, when planned and managed properly, to improve productivity and reduce costs to government;
- information and technology are strategic enablers of quality government service delivery;
- the management and business principles applied to other government resources should be applied to information and technology resources; and
- the private sector is to play a major role in supplying services for the development and support of information technology.

12.2.2 IM/IT Governance

As Chief Information Officer and technology strategist for major government information and technology initiatives (see CPPM chapter 2 section 2.4.1, Central Agency Policy Responsibility Areas) the Office of the Government CIO is the central authority for the government of British Columbia responsible for Chapter 12. The policies contained in this section should be considered in conjunction with other core policy areas on planning (chapter 3), procurement (chapter 6), fees and licensing (chapter 7), asset management (chapter 8), financial systems and controls (chapter 13), risk management (chapter 14), general security (chapter 15), business continuity (chapter 16) and loss management (chapter 20).

The Office of the Government CIO also maintains four major manuals that support the Core Policy and Procedure Manual (CPPM) Chapter 12. They are the:

- Information and Technology Manual (Supplement to CPPM Chapter 12);
- Freedom of Information and Protection of Privacy Policy and Procedures Manual;
- Recorded Information Management Manual; and
- Information Security Policy.

Additionally there are a variety of standards, directives and memoranda that support core policy located on the Government CIO's website.

In May 2006 Cabinet "Mandate[d] the Chief Information Officer with governance authority for standards setting, oversight and approvals for the Province's information and communications technology." The following authorities, responsibilities and accountabilities reflect past ones that have been ascribed to the Government CIO and new ones that have been developed as part of the Government CIO's Governance Working Group's work. They also include authorities, responsibilities and accountabilities ascribed to Ministries and/or Ministry CIOs in the past version of this chapter as well as those recommended through the work of the Government CIO's Governance Working Group.

Government Chief Information Officer

The Government CIO develops, proposes, and maintains corporate-wide IM/IT policy, procedures and standards, and evaluates compliance. Areas associated with this authority include data access, electronic identity management, records management, information management, information technology, privacy, security applications, and systems of government.

Governance and Policy:

a) Legislation

- Recommends legislation in the areas of information and technology management, including access rights in the public and private sector, privacy, security, records management and electronic service delivery.
- Ensures the legislated Personal Information Directory summaries in the Personal Information Directory are maintained.

b) Policies, Procedures, and Standards

- Proposes corporate IM/IT architecture and related policy, procedures and standards to protect and manage information as a government asset.
- Ensures the privacy and security of citizens through the policies, procedures and standards governing citizens' information held by the Province.
- Ensures government's information systems are designed to be interoperable, secure, and able to authenticate and authorize appropriate access.
- Ensures ministries procure information and technology management goods and services compatible with the government infrastructure.
- Clarifies the interpretation of corporate IM/IT policies, procedures and standards.

c) Compliance Monitoring

- Develops mechanisms and processes to ensure compliance with corporate IM/IT policies, procedures and standards.

- Proposes corporate IM/IT performance metrics that enable ministry compliance.
- Informs ministry CIOs of their responsibilities in complying with corporate IM/IT policies, procedures and standards.
- Recommends and reviews audits in coordination with other central authorities to ensure compliance with corporate IM/IT policies, procedures and standards.
- Accesses audit report data to identify information management practices, and information system infrastructure and applications.
- Identifies information necessary for the performance of the Government CIO's duties from any public officer.

d) Advising Government

- Advises senior ministry decision makers, committees and councils, Treasury Board and Cabinet regarding telecommunications, access rights in the public and private sector, privacy, information and technology management, records management, security and electronic service delivery.
- Provides analysis and recommendations to Treasury Board Staff on initiatives, submissions and/or proposals related to information and technology management.

Strategic IM/IT Planning:

a) IM/IT Planning Framework

- Leads the strategic planning process for corporate IM/IT governance.
- Develops, maintains and facilitates the implementation of an integrated government-wide IM/IT planning framework.
- Facilitates the corporate strategic IM/IT planning process and ensures the alignment of IM/IT plans with government's strategic direction.
- Develops and maintains working relationships with Broader Public Sector (BPS) CIOs to communicate government's IM/IT strategic direction and promote the alignment of BPS IM/IT with core government.
- Ensures that the Province is aware of and keeping pace with legislation, policy trends and issues in other jurisdictions.
- Defines corporate vendor engagement strategies to deliver government's IM/IT priorities.

b) Information Resource Planning

- Provides leadership and strategic direction to ministries for the development of the annual Information Resource Management Planning (IRMP) process.
- Coordinates ministry IRMPs with government's IM/IT strategic directions and priorities.

c) IM/IT Human Resource Capital Planning

- Recommends the strategic direction for human resource capital needed to focus on IM/IT functions across government.
- Identifies human, financial and technical resources required to deliver corporate IM/IT strategic plan.
- Advises Public Service Agency on IM/IT human resource capacity required to achieve government's IM/IT strategic directions and priorities.
- Ensures that awareness and training activities inform staff and contractors of their rights, roles and accountabilities for the security, privacy and management of government's IM/IT assets.

Strategic Infrastructure Development:

- Defines the technological direction and framework for IM/IT across government.
- Provides the strategic direction for cross-ministry IM/IT projects.
- Evaluates new information technologies to determine applicability to government business processes.
- Ensures that structures and reporting relationships for IM/IT sub-committees support strategic infrastructure development. Reviews the IM/IT implications of agreements involving compatibility with government's IM/IT infrastructure and strategic directions.
- Designs strategic infrastructure and coordinates activities to enable stakeholder participation in development of the next generation government network.
- Closes the Digital Divide for First Nations communities, and establishes the basis for implementing the next generation government network.
- Provides leadership and obtains resources for key IM/IT projects to facilitate the ongoing development of government's strategic infrastructure.

Transformational Opportunity Analysis:

- Chairs the CIO Council.
- Advises ministries on the hiring of the ministry CIO.
- Researches and reports on transformational activities and leading IM/IT practices in other jurisdictions.
- Identifies and assesses transformational or integrating IM/IT opportunities in government and, where requested, in the Broader Public Sector.
- Promotes the development of cross-government business processes and an enterprise architecture.
- Ensures alignment to the government's strategic direction for major IM/IT projects and projects with service integration implications through project milestone sign-offs and final project approvals.
- Proposes efficiency and effectiveness measures for improvements in the application of information and technology.

Security:

- Provides the overall strategic direction and policy for securing government's information technology infrastructure and government records including electronic information.
- Ensures that measures are established to assess compliance with IM/IT security policies, procedures and standards.

Ministry Chief Information Officer

Governance and Policy:

a) Governance Authority

- Reports to their respective ministry ADM accountable for IM/IT, with a functional reporting relationship between the Government CIO and the ministry CIO.
- Maintains accountability for all business and operational IM/IT initiatives that have no cross-government implications.
- Maintains accountability for IM, budgets, records management, forms management, privacy, security, e-services, business architecture, ministry applications, information management, IM/IT strategic planning and IT (including ministry infrastructure).
- Manages information and technology, and all related support activities.
- Ensures that the delegated responsibility for information and technology is carried out fully.
- Develops an IM/IT workforce strategy to support business transformation, information protection, business continuity and succession planning in consultation with the ministry Strategic HR Director.

b) Legislation

- Provides legislated Personal Information Directory summaries for the Personal Information Directory.

c) Policies and Standards

- Reinforces IM/IT core policies and standards from a risk management perspective.

d) Compliance Monitoring

- Ensures compliance with the IM/IT core policies and standards.

e) Advice to Government

- Ensures that information technology plans address human resource requirements in terms of job design, training and working environment.

Strategic IM/IT Planning:

a) IM/IT Planning Framework

- Establishes strategic direction, consistent with overall government IM/IT direction.
- Participates in ministry service plans and corporate IM/IT planning.
- Accesses the Executive table of each ministry, with stronger emphasis on strategic discussions, rather than just operational issues.

b) Information Resource Planning

- Plans the three year Information Resource Management Plan.
- Works together with other ministry CIOs on horizontal initiatives, both within and across sectors, and adapting to changing priorities.

c) IM/IT Human Capital Planning

- Develops staff to make safe, effective and efficient use of information and technology.
- Manages ministry information resources, ensuring that sound information management practices are followed.

Transformational Opportunity Analysis:

- Provides business analysis and project management expertise.

Strategic Infrastructure Development:

- Functions with a greater role in Information Management within their ministry.
- Supports ministry line of businesses applications.
- Supports ministry-unique applications.
- Develops ministry specific applications if and when required.

Security:

- Protects information holdings in all physical, electronic and digital formats commensurate with its value and sensitivity at all stages in the life cycle of the activity to preserve the confidentiality, integrity, availability, intended use and value of all records.
- Uses security categories approved by Risk Management Branch.
- Identifies and categorizes information and other assets based on the degree of injury (low, medium, high).

12.3 Policy

12.3.1 Appropriate Use of Government Resources

Objectives

- Meet the requirements mandated by the Standards of Conduct.
- Maximize productivity and prevent risks to network security and performance.
- Protect the privacy, confidentiality and security of government's information.
- Increase adherence to government information and technology-related legislation, policies and standards.
- Promote public trust in government's use of information and technology assets.

General

All users of government's information and information technology resources must take responsibility for, and accept the duty to, actively protect them. Government information helps to enable citizen-centric service delivery and information technology supports employees to work efficiently in delivering those services. Proper use of these technologies assists in the daily management of information, saves time and money, reduces administrative overhead and improves service delivery. Improper use may jeopardize the confidentiality, integrity and availability of government information and information technology assets, and may put personal information protection, security or service levels at risk. See the OCIO website for **Appropriate Use of Government Information and Information Technology Resources ("Appropriate Use Policy")** at http://www.cio.gov.bc.ca/cio/appropriate_use/index.page

12.3.2 Information and Technology Planning

Objectives

- Establish planning tools to integrate government's strategic information and technology directions, ministry service plans, and information management and information technology plans.
- Help ministries align information and technology investments with program objectives, and improve services to the public.
- Improve accountability on information and technology initiatives.
- Evolve an enterprise architecture plan that supports the information and technology needs of government.
- Provide strategies for managing information and technology during daily operations, including critical incidents management.
- Facilitate the re-establishment of operations during, and immediately following, a critical incident or other serious disruption.

General

The Office of the CIO oversees the information and technology planning cycle to locate, foster and monitor key issues, opportunities and investments in e-government infrastructure and services. The Government CIO has overall responsibility for the Information Resource Management Planning (IRMP) process. This annual planning cycle is driven by the broader business planning cycle of the government (see CPPM chapter 3, Part 1, Objectives). The development of an IRMP helps ministries align information and technology investments with government strategic plans, ministry service plans, information management and technology plans and program objectives to provide improved services to the businesses and citizens of British Columbia. The IRMP provides an opportunity to assess and strategize for optimization of shared services and consider or implement alternate service delivery approaches.

Vital records and business continuity planning is another key planning area that ensures government's business will continue by keeping information safe and accessible and timely recovery of operations following a service disruption. Plans must include how to re-establish the systems and records that enable government to operate effective and efficiently. Service disruptions can range from a short term inability to access records or services to more significant longer term critical incidents where entire networks may be affected.

Policy

a) Information Resource Management Plans

1. An update of a three to five year Information Resource Management Plan must be submitted annually to the Government Chief Information Officer and Treasury Board Staff.

b) Vital Records and Information Technology Business Continuity Plans

1. Government must create and maintain a business continuity plan that includes identification and management of its vital records.
2. Vital records must be maintained so that re-establishing the legal, financial and functional responsibilities of government is achieved quickly after a catastrophic event or crisis.
3. Vital records must be maintained in a manner that meets current environmental and security standards.
4. Ministries must develop, or work with their supporting infrastructure technology service providers to develop, Business Continuity and Disaster Recovery Plans on all information systems and the associated technology infrastructure and test them regularly.

   See CPPM chapter 16 Business Continuity Management, and chapter 14 Risk Management.

12.3.3 Information Management

Part I: Data Management and Architecture

Objectives

- Derive maximum business benefit from information and technology.
- Facilitate and enhance government's ability to make informed decisions.
- Improve the accuracy and timeliness of data.
- Increase system effectiveness and efficient access to data.
- Share data within legislative authority to improve service delivery to citizens of British Columbia.

General

To demonstrate that services are delivered efficiently and effectively, government must have access to the data in various computer systems, files and reports. Consistent data management practices allow a common structure for data access, integrated programs/services, data sharing and interoperability with government information systems. The use of data within government is governed by legislation that applies to all public bodies. More specific legislation also authorizes ministry program management and information collection including, in some cases, personal information.

Policy

a) Data Management

1. The Government CIO must define, maintain and publish government data definitions and structures to maximize the business value of shared data.
2. Data and corresponding information systems must be identified, classified, inventoried, documented and maintained throughout their lifecycle.

3. Ministries must establish and maintain a data administration/architecture program to manage the design, integrity, availability, and efficient use of data and information systems.
4. Data and corresponding information systems must have an identified Data Custodian.

See Data Administration Standards.

Part II: Personal Information Protection

Objectives

- Ensure the lawful collection, use, retention, disclosure, disposition and security of personal information by public bodies within British Columbia.
- Assure citizens that privacy principles are being taken into account during the design, implementation and evolution of programs, systems and services.
- Ensure that Privacy Impact Assessments are completed and that privacy issues that arise through these assessments are dealt with prior to implementation.
- Ensure that Information Sharing Agreements are completed when a ministry shares personal information with a party external to the ministry.
- Record summaries of Information Sharing Agreements, Privacy Impact Assessments and Personal Information Banks in the Personal Information Directory.

General

To promote government accountability and protect personal information privacy as described in the *Freedom of Information and Protection of Privacy Act* (the Act) all public bodies must comply with the provisions of the Act and its regulation. The FOIPPA Policy and Procedures Manual is a supplemental manual (publicly available) that interprets the Act by describing the operational policies and procedures that ministries and other government offices must use in carrying out their legislated responsibilities. In some cases public bodies may have other legislation specific to their business that adds privacy, confidentiality or security provisions regarding personal information management, (e.g., *Medicare Protection Act*).

Two standard tools that assist ministries in the management of personal information are Privacy Impact Assessments (PIA) and Information Sharing Agreements. Ministries are required to conduct a PIA for new or revised projects, programs, applications, systems or new enactments. The PIA process determines if the privacy protection requirements of the Act are met. In all cases part 1 (basic information) of the PIA should be completed to assess whether personal information is being collected. Where it is determined that personal information is collected the complete PIA is required, whereas if it is not being collected then only part 1 is required. The PIA supports government business objectives by ensuring the collection, use, retention, disclosure and security of information is conducted consistent with the Act and government policies, procedures and protocols. Information Sharing Agreements establish relationships, responsibilities, security requirements, access rights, and authentication requirements between ministries and the data consumers to whom they supply government information. Information Sharing Agreements may also be used in conjunction with alternate service delivery data management contracts and privacy protection schedules or with research agreements to clarify responsibilities of all of the involved parties.

The Act requires that the Minister Responsible for this Act must maintain and publish a Personal Information Directory (PID) to provide summary information about records in the custody or under the control of ministries of the government of British Columbia and about the use and disclosure of those records. The IM/IT Privacy and Legislation Branch of the Government CIO's office (see Information and Privacy) maintains the central directory of Personal Information Banks, Privacy Impact Assessments and Information Sharing Agreements created by and/or operating on behalf of provincial ministries. Ministries as custodians of the data have the knowledge of the personal information holdings and the responsibility to supply the summaries for inclusion into the PID in a timely manner.

To ensure a proactive privacy framework, sound principles of privacy, security and confidentiality must be understood by all users of personal data and incorporated into daily practice within public bodies. This involves developing a culture where privacy is seen as a design objective for information and technology not an obstacle to be overcome. Personal privacy is a right protected through legislation, policies and best practices by the Government of British Columbia.

Policy

a) Privacy Impact Assessments

1. A Privacy Impact Assessment (PIA) must be conducted to determine if a project, program, application, system or new enactment collects, uses, retains or discloses or secures personal information.
2. A preliminary PIA must be completed during the feasibility or initiation stage of any project, program, application, system or enactment. A formal PIA must be finalized, including the sections on security and retention of personal information, before implementation of any project, program, application, system or enactment.
3. Ministries must review existing summaries in the government Personal Information Directory, PIA section, at least once a year, and submit new summaries as needed within 30 days of the final signing off of a PIA.

b) Information Sharing Agreements

1. Ministries must develop Information Sharing Agreements to cover personal information exchanges outside of the immediate program area, as required. These agreements must include a compliance review requirement and schedule of planned reviews.
2. Ministries must review existing sharing agreement summaries in the government Personal Information Directory, Information Sharing Agreement section, at least annually, and submit new summaries as needed within 30 days after approval of an Information Sharing Agreement.

c) Personal Information Banks

1. Ministries must maintain a directory of Personal Information Banks and review the existing Personal Information Banks summaries in the government Personal Information Directory at least annually.
2. New Personal Information Bank summaries must be submitted to the government Personal Information Directory within 30 days of implementation.

d) Personal Information Management

1. People who manage access or use government information must receive privacy and information management training on initial employment and as required thereafter.
2. Personal information in the custody or control of public bodies must be stored, managed and accessed solely within Canada throughout its lifecycle, except in specified circumstances.
3. Remote access from a foreign country to personal data, including viewing, is prohibited except in specified circumstances.
4. Ministries must use the principles of "need-to-know" and "least privilege" when authorizing access to personal information.

Part III: Managing Information

Objectives

- Assign responsibility and accountability for the management of information within the custody, or under the control of, government.
- Assure compliance with legislation, policies and standards.
- Create and retain a full and accurate record documenting decisions and actions.
- Provide relevant information in a timely, useable, cost-effective, and accurate manner.
- Preserve government information in a manner that retains the information's authenticity, reliability, accessibility and integrity for as long as required.
- Support transparent and effective access to government information within legally established privacy and confidentiality restrictions.

General

The *Interpretation Act* definition of "record" includes all recorded information, whatever the media or format. Information management is a core component of government infrastructure and ensures that critical characteristics such as authenticity, reliability, integrity and usability of a record are preserved and protected for as long as required.

Government must appropriately provide access to, manage, preserve and dispose of its records in compliance with the *Document Disposal Act*, the *Freedom of Information and Protection of Privacy Act*, and other relevant legislation, policies and standards, in order to:

- ensure government accountability;
- provide evidence of its activities and organizational structure;
- document its responsibilities, rights and entitlements; and
- preserve records of enduring value.

Records deemed to have enduring value will be preserved in the government archives. Government records are eligible for final disposition when their scheduled active and semi-active retention periods have expired.

The Government of British Columbia standards for the classification and scheduling of its records are documented in the Administrative Records Classification System (ARCS), the Operational Records Classification Systems (ORCS), ongoing records schedules and other approved records schedules. ARCS and ORCS support the automated scheduling and classification of records within an Enterprise Document and Records Management System (EDRMS). The implementation of the government standard EDRMS software in conjunction with other digital preservation practices and procedures (e.g., storage and media management, metadata standards) supports government's requirements for long-term records preservation.

Policy

a) Governance of Recorded Information

1. Government must manage all records created and received during the conduct of its business activities.
2. Ministries must establish and maintain a recorded information management program.
3. Ministries must establish and maintain a forms management program.
4. Government records must be managed and preserved to remain authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format.
5. Ministries transferring records to off-site storage must use approved records centres.

See CPPM chapter 15, Security.

b) Classification, Scheduling and Maintenance of Government Records

1. Ministries must implement and maintain the government standard records classification and scheduling systems (i.e., ARCS, ORCS, Ongoing Records Schedules).
2. Ministries must develop records classification systems for their operational records (ORCS).
3. Ministries must use the government standard Enterprise Document and Records Management System (EDRMS) when implementing an electronic document and records management system.
4. Government records must remain authentic, reliable and accessible after any conversion or migration from one media, format, or system to another.

c) Storage and Disposition of Government Records

1. Government records must be disposed of securely in accordance with approved records retention and disposition schedules and asset management processes.
2. Ministries must establish internal records disposition procedures.
3. Government records scheduled for archival retention must be maintained in a manner that preserves their integrity and authenticity up to and throughout transfer to the government archives.
4. Government records scheduled for destruction must be destroyed in a method appropriate for the recording media and that maintains the security of the information and the privacy of individuals.

See CPPM chapter 6, Disposal of Surplus Assets, chapter 8, Asset Management and chapter 20, Loss Management.

d) Working Outside the Workplace

1. Reasonable security measures must be made to safeguard electronic storage devices and paper-based confidential and/or personal information while in transport and in use outside the workplace.
2. The most appropriate electronic method for accessing confidential and/or personal information must be established prior to working outside the workplace in accordance with the Working Outside the Workplace Policy.
3. Confidential and/or personal information must not be downloaded/stored to a non-government computer or other device (for example, smartphone, memory stick/card, external hard drive, etc.).

See the Working Outside the Workplace Policy

Part IV: Sharing of Government Information

Objectives

- Adhere to government strategic directions for information management.
- Respond to citizens' needs and expectations of connecting with government electronically, and increasing government accountability to the public.
- Improve ministry products, services and programs.
- Enhance understanding of information used to make decisions.
- Promote efficient and effective sharing while leveraging experience and knowledge of data already collected within government.
- Exchange personal information between a public body and a person, a group of persons or an organization, as allowed within privacy and ministry-specific legislation regarding personal information.

General

Government information is an asset that may be under the custody or control of a ministry or other government agency but is collected for, and owned corporately by, the Crown, i.e., the Province. To achieve the government's goal of effective and efficient citizen-centred service delivery, and to improve public service outcomes, the sharing of relevant information by authorized users must be done across service teams and for common or integrated programs. Sharing of information must be allowed under the *Freedom of Information and Protection of Privacy Act* or another enactment prior to disclosure. The authorized and appropriate use of information within government benefits the citizens and the Government of British Columbia. In particular:

- Routine release is the disclosure of information held by a public body without the necessity of a more costly formal Freedom of Information request.
- Contacting government electronically is becoming a normal part of communications between government, businesses and citizens in British Columbia. An employee's work email address is defined in the *Freedom of Information and Protection of Privacy Act* as contact information and is not therefore personal information. However, the release of a government email address may be restricted in cases involving employee health and safety issues.
- Legally mandated information-sharing requests, e.g., where requirements to disclose information for legal cases or Inquiries, are to be addressed to the appropriate ministry solicitor, Legal Services Branch.

Policy

a) Routine Release of Information

1. Ministries must promote the routine release of information, where allowed by the Freedom of Information and Protection of Privacy Act.
2. Ministries may charge fees for information made available routinely, as pre-approved by Treasury Board.

b) Internal Use of Government Information Assets

1. Originating ministries providing information to internal-to-government users must not charge for information in its basic format. The originating ministry is to determine the basic format for the information. Special circumstances to be negotiated between the two parties.
2. The originating ministry must allow access to information for internal-to-government users in its basic format in the most cost-effective manner (e.g., intranet website). Information access costs are to be borne by the requesting ministry.
3. The information held by the originating ministry must be considered the correct or official version. Internal-to-government users must ensure that the most current version of information be used.
4. Requesting ministries do not have the right to reproduce, market or distribute information to external-to-government users without the approval of the originating ministry. Originating ministries should develop and provide liability disclaimers appropriate for the information being disseminated.
5. To protect confidentiality and security, the information being shared must be documented and shared only on a need-to-know and least privilege basis.

See CPPM chapter 7, section 7.3.2 Fees and Licenses, Privacy Protection Schedule (PPS) and Procurement, Part I, 6.3.3.e, Administration, policy 12.

c) Publication of Government Email Addresses

1. Government email addresses, including generic office email addresses, must be kept up to date and published in the British Columbia Government Directory except where exempted for health and safety reasons.
2. Generic office email IDs may be used when required to meet operational requirements. A specific, designated owner must manage each generic office email ID.
3. Individual alias email IDs must not be used.
4. Government email addresses must not be made available electronically in bulk form external to government (e.g., electronic files, distribution lists).
5. Government e-mail addresses must use the government naming convention (i.e.,firstname.surname@gov.bc.ca) and must not include a host name.

d) Disclosure Requirements for Legal Proceedings

1. Ministries must list all relevant records in their custody or control under the Attorney General's discovery of documents.
2. Government records destruction schedules must be suspended during court orders for Demand of Discovery.
3. Records disposition must be suspended during legally mandated reviews (e.g., litigation, document discovery, and commissions of inquiry.)

e) Crown Copyright

See CPPM chapter 6 Procurement, section 6.3.4.e, Crown Copyright.

f) Intellectual Property

See CPPM chapter 6 Procurement, section 6.3.4.f., Disposal of Intellectual Property.

12.3.4 Electronic Identity Management

Objectives

- Interact electronically with businesses and citizens to conduct business transactions.
- Facilitate the legal use of electronic signatures in e-services between government and citizens and businesses.
- Provide assurance to users of e-services that the privacy, confidentiality, integrity and security of their information will be maintained to the highest possible standard.
- Promote public confidence in management of the identity and eligibility information used for government electronic service delivery.

General

BC government strategic direction includes a commitment to integrate services and to deliver them electronically where possible. This strategy supports a client-centric framework that will assist and enable ministries to deliver services better through improved access to business and citizen online services.

To enable electronic service delivery, the BC government passed the *Electronic Transactions Act* to support its move into the global electronic economy. The principle purpose of the Act is to provide legal equivalence between paper and electronic documents and signatures, except in limited circumstances.

Identity management consists of a number of processes that include:

- registration and issuing of electronic identities and credentials;
- identity proofing - how government proves an individual is who they claim to be;
- authentication - how government knows a user is who they claim to be when accessing services online;
- authorization - decisions about what services an individual is eligible for; and
- access controls - controls around what information a user will see and how users' views will be managed.

Policy

a) Electronic Signatures

1. Ministries must consider the benefits of using electronic signatures in all e-service initiative designs, and choose the manner of signature(s) that best serves the initiative.

b) Identity Management

1. All users must have a unique application user logon profile.
2. Government e-services requiring user authentication must use the Enterprise Security Gateway for authentication, unless an exemption has been granted by the Government CIO.

12.3.5 Information Technology Management

Objectives

- Promote the principles and best practices of project management in all information and technology projects.
- Provide a context for overall government direction within which ministries can establish their information and technology architecture directions.
- Maximize information technology system to system and human to system interoperability.
- Maximize effectiveness and efficiency of information technology implementation and operations.
- Encourage compatibility and supportability across the government's information and technology environment.
- Lower service costs to government through effective information technology procurement practice.
- Optimize the use, performance and cost of information technology resources.

General

In British Columbia government strategic direction includes a commitment to integrate services and to deliver them electronically where possible. This strategy supports a client centric framework that will assist and enable ministries to deliver services better through improved access to business and citizen online services.

Professional project management is the basis for developing sound strategic and operational information and technology initiatives. Project management includes incorporating best practices, standards and proven methodologies to foster a consistent formal approach that maximizes success in information and technology initiatives.

Corporate information technology standards serve as a "building code" to provide client centered services regarding interoperability, efficiency, security and privacy while recognizing that the least amount of regulation promotes innovation and where appropriate, competition. This will result in some standards being high-level (e.g., statements of best practices, industry standards, and recognized leading methodologies) while others, of necessity, will be at a lower level (e.g., services, products, or tools).

The purpose of corporate shared services is to employ best practices in cost control, optimizing return on investments, implementing standardization and improving the effectiveness and efficiency of services, products and tools. The Government CIO has authority to identify where a corporate approach should be used in planning for shared services, new initiatives and procuring information and technology assets. (see CPPM Chapter 6, section 6.3.5 a, Information Management and Information Technology Procurement).

Evaluations provide assurance to Treasury Board, the Government CIO and senior ministry management that information technology best practices, policies, standards and guidelines have been implemented and are functioning effectively across government. Routine evaluation of information technology is a change management methodology that impacts daily operations, service delivery planning, modifying existing systems or implementing new systems, and forms a key component of Enterprise Risk Management feeding into the annual business planning cycle.

Policy

a) Information and Technology Project Management

1. Responsibility for the management and control of information and technology projects resides with executive-level program management through the annual IRMP process.
2. Ministries must select a methodology for the development of information systems appropriate for the size, complexity, nature and cost of the development project.
3. A Project Steering Committee must be established to provide direction and decision making for any high-risk major development project.
4. Major information and technology projects must be monitored against a documented master project plan.
5. Post Implementation Reviews must be done on all major projects.
6. Development of information systems must be conducted by the private sector unless an exemption is granted by the Government CIO.
7. Information system application plans that will use or interface with a shared computer facility or service must include a government-wide approach and, where available, use shared services to achieve economies of scale in the use and management of information and technology.
8. Development of new financial systems or enhancements, changes or revisions to existing ones must be formally approved in accordance with CPPM chapter 13, Financial Systems and Controls.
9. Development of new electronic commerce systems or enhancements, changes or revisions must be formally approved by Banking & Cash Management to ensure compliance with payment card industry (PCI) standards.

See CPPM chapter 7, section 7.3.8 - Acceptance of Electronic Payments, and the IM/IT Standards Manual.

b) Information Technology Standards

1. Standards and exemptions from published standards, must be approved by the Government CIO.
2. Standards must support the efficient, secure operation of systems while maintaining privacy.
3. Standards must provide the least amount of regulation to promote innovation and competition, where appropriate.
4. Standards must maximize effectiveness and efficiency for information technology planning, design, implementation and operations.

c) Information and Technology Procurement and Unsolicited Proposals

1. Government-wide approaches and standards must be used in information and technology asset procurement and in managing unsolicited information and technology proposals by vendors.

See CPPM chapter 6, section 6.3.5, Information Management and Information Technology Procurement.

d) Information Technology Operations and Evaluation

1. Ministries, in conjunction with Workplace Technology Services, must establish and maintain inventories of computer hardware, software and related communications equipment.
2. Ministries must identify a funding source in the annual ministry information technology plan for the evaluation of compliance, system or security controls identified for a project, system or application.

See CPPM chapter 8, Asset Management and chapter 20, Loss Management.

12.3.6 Information and Technology Security

Objectives

- Ensure appropriate security measures are established for all data, information, applications, hardware, associated documentation and computer facilities.
- Support incorporation of privacy principles in the design of information systems.
- Support access to data, software and computer facilities, based on demonstrated need and authorization.
- Ensure information is viewed and managed as an asset that must be protected commensurate with its value.
- Select only those vendors who will undertake to comply with the security policies of this chapter when contracting for data processing services or engaged in alternate service delivery initiatives.

General

Security is the responsibility of all employees, contractors and others who have access to, use or manage the information and technology assets of government. Information systems security includes the protection of personal data, systems, documentation, computer-generated information and facilities from accidental or deliberate threats to confidentiality, integrity or availability. Security policies apply to all locations where information is processed or stored by, or on behalf of government (e.g., Workplace Technology Services, ministry and contracted computer facilities).

Policy

a) Security

1. A formal management framework will be established to initiate, implement, monitor and enforce information and technology security within the Government of British Columbia.
2. Security requirements must be assessed, identified and documented to determine security implications and control requirements when there is a requirement for third parties to access government assets. Security controls must be documented and agreed to with the third party.
3. Information and technology assets must be classified, inventoried and recorded with an identified owner who is responsible for achieving and maintaining appropriate protection of those assets.
4. Users of government assets must continue to be aware of, and understand, their role in reducing the risk of theft, fraud or misuse of government assets. Changes in responsibilities, roles, contracts or employments must be managed.
5. Operating procedures must be documented and monitored to ensure the correct and secure operation of information and communication technologies.
6. Third party service delivery agreements must be monitored for compliance, and changes managed to ensure that the services delivered meet or exceed specified requirements.
7. Operational requirements for new systems must be established, documented and tested prior to acceptance and use. Future capacity requirements should be made to reduce the risk of system overload or failure.
8. Documents, computer media, data and system documentation must be protected from unauthorized disclosure, modification, removal or destruction.
9. Data and information exchanges within government, or with an external entity, must be secure and managed through a documented process.
10. Government information and technology assets will be monitored regularly and logs maintained to identify inappropriate access, use, or other security events.
11. Access to information, systems, and business processes must be managed and controlled on the basis of business and security requirements.
12. Access to, or from, internal and external networks and network services must be managed and controlled.
13. Security requirements must be assessed, identified, documented, and agreed to during all stages of development.
14. The security controls of new or modified information systems and services must be reviewed prior to implementation.

15. Information and technology assets will be protected commensurate with the identified risks and security requirements.
16. Information security incidents, events and weaknesses must be managed and communicated to the Government Chief Information Officer for corrective action, if appropriate.
17. Information security management requirements must be integrated into the business continuity planning process to protect information systems and communication technologies from disasters, loss of service or information security failures.
18. The security of information systems and communications technologies must be regularly reviewed to ensure compliance with applicable legislation, policies, standards and documented security controls.

b) Reporting the Loss or Unauthorized Disclosure of Government Information

1. The Government Chief Information Officer is responsible for the coordination, investigation, and resolution of information incidents.
2. All actual or suspected information incidents must be reported immediately using the Information Incident Management Process.
3. The Government Chief Information Officer is responsible on behalf of government, for liaising with the Office of the Information and Privacy Commissioner regarding an actual or suspected privacy breach.

See CPPM chapter 15, Security and CPPM L, Loss Reporting, and the Information Security Policy Manual.

12.4 Information and References

12.4.1 Definitions

Administrative Records Classification System (ARCS) – The government-wide standard for classifying, filing, retrieving and disposition scheduling of administrative records. ARCS also includes freedom of information and protection of privacy designations. ARCS is a block numeric system, reflecting function and subject. See also ORCS.

Application – A collection of computer hardware, computer programs, databases, procedures and knowledge workers that work together to perform a related group of services or business processes.

Attorney General's discovery of documents – A demand for discovery of the documents which are or have been in the party's possession or control relating to any matter in question in the action, and the other party shall comply with the demand by delivering a list of the documents that are or have been in the party's possession or control relating to every matter in question in the action.

Basic format information – information used by the originating ministry to conduct its business. Examples could include raw data or value-added information in either electronic or hard copy formats.

Computer media – An object or device that electronic information is stored on. It includes, but is not limited to, tapes, disks, diskettes and computer hard drives.

Court ordered for Demand of Discovery – The court may order that a party deliver a list of the documents that relate to a matter in question in the action to any other party and that, although not in the possession or control of the party against whom the order is made, are within that party's power.

Data – The data that is an individual fact (datum) or multiple facts (data), or a value, or a set of values, but is not significant to a business in and of itself. Data is the raw material stored in a structured manner that, given context, turns into information.

Data Custodian – A senior manager for a business area responsible for data requirements, standards, access rules, business training, etc. They define the business value, scope, standards and services of the organization's data within the context of their mandate.

Electronic Signature – Information in electronic form that a person has created or adopted in order to sign a record and that is in, attached to, or associated with, the record.

Government – Any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of British Columbia.

Government records – All records, regardless of physical format, that are received, created, deposited, or held by or in any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of British Columbia.

The Interpretation Act (RSBRITISH COLUMBIA 1996, c. 238, s. 29) defines "record" as follows: "'record' includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise."

Government records consist of records in every physical format, including electronic records, film, audio and audiovisual tapes.

Government records include cabinet ministers' records that are created and/or accumulated and used by a minister (or a minister's office) in developing, implementing and/or administering programs of government. Government records do not include legislative records.

The retention and final disposition of most government records is governed by the Document Disposal Act. See also Executive records, MLA records, Non-government records, Personal records.

Host Name – Any name that is included in an email ID that can be used to identify the network address of a computer.

Information – The data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision-making. The finished product as a result of the interpretation of the data.

Information Incident - a single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information. Information incidents include privacy breaches (see the Process for Responding to Privacy Breaches). 12.3.6

Information and Technology Resources – Information and communications technologies, including data, information systems, network services (e.g., web services; messaging services); computers (e.g., hardware, software); telecommunications networks, and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants).

Information Management – The application of systematic planning, controls and standards to the creation, use, transmission, retrieval, retention, conversion, final disposition, and preservation of information resources in all formats, and the improvement of information handling systems of all kinds.

Information System – A system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output and control functions in relation to information and data. Normally used to describe computerized systems, including data processing facilities, data base administration, hardware and software which contain machine-readable records. A collection of manual and automated components that manages a specific data set or information resource.

Information Technology – The common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services.

Internet – The global interconnection of data networks or bulletin board systems that commonly use (but are not limited to) the Internet Protocol.

Least Privilege – A security 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. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Major Project – A project that is over six months duration or identified as high risk or cost greater than or equal to $250,000.

Master Project Plan – A document that describes the common vision of the project, the overall project management functions, specific deliverables and establishes the detailed project workplan and budget.

Need-to-know – A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office.

The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on automated information systems.

The need-to-know principle is especially important in protecting the privacy of individuals as required by the *Freedom of Information and Protection of Privacy Act*.

Ongoing records schedule – A records schedule that authorizes the retention and final disposition, on a continuing basis, of the types of records described in the schedule. ARCS and ORCS serve as ongoing records schedules for ministry or agency administrative records and operational records. Special records schedules are another type of ongoing records schedules.

Operational Records Classification System (ORCS) – An integrated records classification and scheduling system tailored to the operational records of a specific function or program of government, in accordance with government-wide standards. ORCS facilitate classification, filing, retrieval and disposition; ORCS may also be used to identify vital records and freedom of information and privacy designations. ORCS is a block numeric records classification system, reflecting function and subject.

Originating ministry – The ministry or agency which is the prime or original holder of the information.

Payment Card Industry (PCI) Standards – payment systems standards issued through the international Payment Card Industry Security Standards Council and required by the payment card industry.

Record – Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.

Requesting ministry – The ministry or agency requesting information from the originating ministry. This policy will use the term "information" to encompass raw data, summaries, abstractions, consolidations and other products derived from data.

Routine Release – The disclosure of certain types of information as a matter of course without the necessity of a formal Freedom of Information (FOI) request. Routine release includes, but is not limited to, the release of records that have been designated as available without a formal request under section 71 of the Act. Routine release may be reactive (responding to requests for information when received) or proactive (systematically disseminating information in advance of requests using mechanisms such as the Internet, libraries, etc.).

Security event – An identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

User – Persons (including employees and contractors) authorized to access and/or use government information technology resources.

Vital Records – The records of government that contain information essential to:

- conduct of emergency operations during and immediately following a disaster;
- resumption/continuation of government services or operations;
- re-establishment of the legal, financial and functional responsibilities of government; and
- re-establishment of the rights and obligations of individuals, corporate bodies and other governments with respect to the Government of British Columbia.

12.4.2 Links

The following links will provide the reader with additional details and guidelines from the Office of the Government CIO information management and information technology policies and standards, directives and memos, key support manuals and information technology security.

1. Legislation
    a. *Freedom of Information and Protection of Privacy Act* and Freedom of Information and Protection of Privacy Regulation (B.C. Reg. 323/93)
    Personal Information Protection Act and Personal Information Protection Act Regulations (B.C. Reg. 473/2003)
    Electronic Transactions Act
    b. *Document Disposal Act*

2. Branches

    Knowledge and Information Services Branch
    http://www.cio.gov.bc.ca/cio/kis/index.page?/

        Freedom of Information and Protection of Privacy Policy and Procedures Manual
        http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page?

    Information Security Branch
    http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?

        Information Security Policy Manual
        http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf

    Information Access Operations
    http://www.gov.bc.ca/citz/iao/records_mgmt

        Recorded Information Management Policy and Procedures Manual
        http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/index.html

    Provincial Treasury Banking & Cash Management - PCI DSS Resource Centre
    http://gww.fin.gov.bc.ca/gws/pt/bcm/bankPCI.stm (government access only)

Print and Close Cancel