INFORMATION SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 2.0
Published: September 2019

Replaces Version: 1.0
# Table of Contents

1 Introduction .................................................................................................................. 3

II Scope ............................................................................................................................. 3

III Background .................................................................................................................. 4

IV Terms and definitions ................................................................................................ 4

V List of commonly used references ............................................................................... 5

1 Information Security Policy .......................................................................................... 6
   1.1 Security Policies – Information Security Policy ..................................................... 6
   1.2 Organization of Information Security ..................................................................... 6

2 Mobile computing and teleworking ............................................................................ 19

3 Human Resource Security ........................................................................................... 19

4 Asset Management ....................................................................................................... 19

5 Access Control ............................................................................................................. 19

6 Cryptography ................................................................................................................ 19

7 Physical and Environmental Security .......................................................................... 19

8 Operations Security ..................................................................................................... 20

9 Communications Security ............................................................................................ 20

10 System Acquisition, Development and Maintenance ............................................... 20

11 Supplier Relationships ............................................................................................... 20

12 Information Security Incident Management ............................................................. 20

13 Information Security Aspects of Business Continuity Management ...................... 21

14 Compliance ................................................................................................................. 21

Appendix A – Glossary ..................................................................................................... 22

Appendix B – List of commonly used references ............................................................ 29
I Introduction
The Office of the Chief Information Officer is responsible for providing information technology infrastructure that enables cost-effective, citizen-centred services. This responsibility includes a requirement to provide reliable and secure IT services.

The Government of British Columbia is the custodian of extensive information holdings and relies upon its information assets for fiscal, policy and program delivery initiatives. The management of public information requires government to protect the confidentiality, integrity and availability of the information assets in its care. Citizen trust in the government’s ability to maintain the privacy and security of their information is essential.

The Information Security Standard (ISS) provides the framework for government organizations to meet their goals to protect government information and technology assets. In addition, the comprehensive Information Security Program, headed by the Chief Information Security Officer, as the Executive Director of the Information Security Branch, supports Chapter 12 of the Core Policy and Procedures Manual.

The Information Security Standard is based on the International Standardization Organization (ISO) 27002:2013 standard for information security management – Information Technology – Security Techniques – Code of Practice for Information Security Controls. This standard provides a structured approach to identifying the broad spectrum of information security activities in the life-cycle of information systems.

The Information Security Standard incorporates a risk-based approach to security using Security Threat and Risk Assessments to consider business process and government service delivery implications; technology implications; and communications strategies including employee information security awareness programs.

Glossary
Appendix A provides a Glossary of key terms in this standard.

II Scope
The Information Security Standard applies to all core government. Contracted service providers conducting business on behalf of government must comply with the Information Security Standard (or demonstrate compliance with ISO 27002:2013) and the other IM/IT Standards. See section V below for a list of references and hyperlinks.

Exemptions from an IM/IT or Architecture Standard may be granted subject to the approval of the Government Chief Information Officer. An Exemption request and supporting documentation for the business need must be submitted to the Government Chief Information Officer for consideration of the exemption. See section V below.
III Background

The Information Security Standard (version 2.0) is implemented concurrent with the implementation of the Information Security Policy (version 4.0) which becomes the new cross-government policy for information security.

Organization of the document
Sections 2 through 14 of this standard and have been partitioned off as independent sub-standards for ease of future updating and maintenance. These sub-standards (sections 2 through 14) are designed to be read in conjunction with section 1 of this standard.

References – a master list of references is included at the end of the document in Appendix B. This eliminates the need of overcrowding the document with repeating reference sections.

IV Terms and definitions
There are some word pairs used in the Information Security Standard that users have found cause confusion and require clarification. Because they do apply to the ISS overall and are used throughout, these word pairs are defined here, apart from the Glossary.

Information Owners vs Information Custodians – “Information Owners” have the responsibility and decision-making authority for information throughout its life-cycle, including creating, classifying, restricting, regulating and administering its use or disclosure. Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister. “Information Custodians” maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. In contrast, information custody means having physical possession of information without necessarily having responsibility for the information.

Must vs Should – The term “must” is defined as an absolute requirement. Policy statements using the word “must” are mandatory. The term “should” refers to a good practice to follow that is advisable, but not strictly required. “Should” means that there may exist valid reasons in a particular circumstance to use alternative solutions, but the implications of an alternative must be fully understood and carefully weighed before choosing a different course from what is in the policy statement.

Standards vs Guidelines – “Standards” refer to industry specific standards, government standards and standardized process documents developed to support a specific policy or requirement. “Standards” are industry-approved specifications for quality that can be measured against. Organizations can exceed the standards but should not fall below them. “Guidelines” refer to recommendations, best practice or support documents and processes that help with the interpretation and implementation of a specific policy or requirement. “Guidelines”, where they are provided, serve to assist someone and offer some direction.
Exceptions vs Exemptions – “Exceptions” refer to specific cases where a certain requirement does not apply. Where for certain reasons a Ministry or a program area cannot comply with a specific requirement, they must request an Exemption. The request submission must be accompanied by a completed Security Threat and Risk Assessment and Privacy Impact Assessment. Exemption requests follow a stringent review process by the Office of the Government Chief Information Officer.

V List of commonly used references

See Appendix B - List of commonly used references.
1 Information Security Policy

The Information Security Policy (Section 1.1) establishes requirements to ensure that information security controls remain current as business needs evolve and technology changes. This policy must be published and communicated to all employees and relevant external parties.

To support the implementation of the requirements in the Information Security Policy, the Organization of Information Security (Section 1.2) provides guidance on the management structure needed to coordinate information security activities, including who coordinates them and what agreements are required.

1.1 Security Policies – Information security policy

1.1.1 The Office of the Government Chief Information Officer is responsible for establishing, issuing and monitoring information security policies.
   a) Information Security Policy
   b) Ministry or agency information security policy

Purpose: To establish comprehensive information security policies, processes and practices that will assist Ministries in delivering services.

1.1.1 a) Information Security Policy

The Information Security Policy contains government requirements for the secure delivery of services. Secure service delivery requires the assurance of confidentiality, integrity, availability and privacy of government information assets through:

- Management and business processes that include and enable security processes;
- Ongoing employee awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Defining security responsibilities;
- Identifying, classifying and labelling assets;
- Ensuring operational security, protection of networks and the transfer of information;
- Safe-guarding assets utilized by third parties;
- Reporting information security incidents and weaknesses;
- Creating and maintaining business continuity plans; and,
- Monitoring for compliance.

The Office of the Government Chief Information Officer recognizes that information security is a process, which to be effective, requires executive and management commitment, the active participation of all employees and ongoing awareness programs.

1.1.1 b) Ministry or agency information security policy

Ministries may develop and implement information security policies, standards and guidelines for use within their organization or for a specific information system or program. Ministry developed information security policies, standards and guidelines can exceed but must not conflict with information security policies and standards established by the Office of the Government Chief Information Officer.
Standards:
In most instances, where standards exist they are referenced in individual policies. All relevant policies, standards and additional resources appear in section V of the Introduction, with hyperlinks. The Office of the Government Chief Information Officer will issue and revise government standards as needed.

Guidelines:
Guidelines may be included to assist in interpretation and implementation.

Recommended Tests:
Note: 1.1.1 is reported on as part of the annual information security review.

- Demonstrate that Ministry awareness programs identify the Information Security Policy.
- Demonstrate employees are made aware of policies that affect their program areas.

1.1.2 The Information Security Policy must be reviewed on an annual basis and updated when required.

a) Information Security Policy review – Office of the Government Chief Information Officer
b) Information Security Policy review – Ministries and other agencies

Purpose:
To ensure information security policies remain current with evolving business needs, emerging risks and technological changes.

1.1.2 a) Information Security Policy review – Office of the Government Chief Information Officer

The Office of the Government Chief Information Officer is responsible for reviewing information security policies, standards and guidelines on an annual basis. Policies and standards reviews must be initiated:

- In conjunction with legislative, regulatory or policy changes which have information security implications;
- During planning and implementation of new or significantly changed technology;
- Following a Security Threat and Risk Assessment of major initiatives (e.g., new information systems or contracting arrangements);
- When audit reports or security risk and controls reviews identify high risk exposures involving information systems;
- If threat or vulnerability trends produced from automated monitoring processes indicate the probability of significantly increased risk;
- After receiving the final report of investigation into information security incidents;
- Prior to renewing third party access agreements which involve major government programs or services;
- When industry, national or international standards for information security are introduced or significantly revised to address emerging business and technology issues; and,
- When associated external agencies (e.g., Information and Privacy Commissioner, National CIO Sub-Committee on Information Protection, RCMP) issue reports or identify emerging trends related to information security.
1.1.2 b) Information security policy review – Ministries and other agencies
Where ministries have developed ministry specific information security policies, standards and guidelines they must review them annually.

Recommended Tests:
Note: 1.1.2 is reported on as part of the annual information security review.
Demonstrate that Ministry specific policies have a development, review and approval process.
1.2 Organization of Information Security
This chapter describes the management structure needed to coordinate information security activities, including who coordinates them and what agreements are required. Coordination of information security activities requires the support of a network of contacts in the information security community to elicit advice, monitor trends and deal with other external factors.

1.2.1 Internal organization

1.2.1.1 Executive must set direction and provide support for information security.

<table>
<thead>
<tr>
<th>Purpose: To establish executive direction on, and commitment to, information security to maintain the confidentiality, integrity and availability of government information.</th>
</tr>
</thead>
</table>

1.2.1.1 a) Executive support for information security
Ministry executives, including Deputy Ministers, Associate Deputy Ministers, Assistant Deputy Ministers, and Executive Directors are expected to promote information security initiatives within their ministries and support the information security activities of the Information Security Program published by the Office of the Government Chief Information Officer.

The Government Chief Information Officer is an Associate Deputy Minister and a member of the Ministry executive. The office is referred to, in branding, as the OCIO, or Office of the Chief Information Officer. Both of these terms apply to the same government entity.

The Information Security Program provides the security foundation necessary to protect government information assets by:

- Establishing an information security architecture for standard security controls across government;
- Defining organizational roles and responsibilities for information security;
- Developing and reviewing the Information Security Policy;
- Monitoring and measuring the implementation of the Information Security Policy; and,
- Developing and delivering a program to maintain information security awareness.

1.2.1.1 b) Chief Information Security Officer
The Chief Information Security Officer must establish an Information Security Program to manage and co-ordinate information security activities across government by:

- Providing leadership on methodologies and processes for information security;
- Establishing a cross ministry information security forum;
- Identifying security controls required to enable government service delivery and documenting those controls in the information security policies, standards and guidelines;
- Providing security-related technical architecture advice to planning and development groups;
- Promoting information security education, training and awareness throughout government;
- Identifying significant threats and exposures associated with information security;
• Ensuring the Information Incident Management Process is followed for all suspected or actual information incidents;
• Evaluating information received during and after an information security incident;
• Implementing performance measurement processes for security controls;
• Ensuring information security activities are in compliance with the information security policies and standards;
• Identifying responses to remediate activities that are not in compliance with policies, standards or best practices;
• Co-ordinating the implementation of information security controls;
• Recommending appropriate actions in response to identified information security incidents and initiating audits where necessary; and,
• Building relationships with stakeholder and partner organizations including suppliers, other provincial security incident response centres and national incident response centres to assist in maintaining the Information Security Program.

Information Owners and Information Custodians must include the Office of the Chief Information Officer and the Chief Information Security Officer, or a designate, as part of the business functions (e.g., security architecture, policy, standards, and security controls requirements) for all corporate shared infrastructure and services, and in the definition of standards and contractual requirements for the procurement of outsourced corporate shared infrastructure and services, to ensure that all controls and protection levels have security by design.

1.2.1.1 c) Information Security Branch support
The Chief Information Security Officer is the Executive Director of the Information Security Branch. Information security specialists in the Information Security Branch, Office of the Government Chief Information Officer, are responsible for:
• Interpreting the Information Security Policy to assist in the delivery of business functions;
• Evaluating information security implications of new government initiatives;
• Performing information system security risk analysis activities;
• Performing Security Threat and Risk Assessments and reviews;
• Evaluating new threats and vulnerabilities;
• Investigating information security incidents;
• Advising on the information security requirements for documented agreements;
• Identifying general business trends and emerging technologies, and recommending changes to the Information Security Program;
• Analyzing and providing advice on emerging information security standards;
• Determining and evaluating security requirements and necessary security controls in relation to corporate risk for corporate shared infrastructure and services, as well as outsourced services;
• Providing information security advice for business areas; and,
• Providing information security education and awareness activities and resources.

Recommended Tests:
Note: 1.2.1.1 is reported as part of the annual information security review.
### 1.2.1.2 Implementation of information security activities across government must be co-ordinated by the Office of the Government Chief Information Officer.

<table>
<thead>
<tr>
<th>a) Security co-ordination across government</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) Security co-ordination within a ministry</td>
</tr>
</tbody>
</table>

**Purpose:** To ensure that information security activities are carried out in a timely manner and that security issues are resolved.

#### 1.2.1.2 a) Security co-ordination across government

A cross-government information security forum will provide advice and recommendations for:

- Developing and implementing information security policies, standards and guidelines;
- Promoting the consistent application of information security programs;
- Identifying issues related to information security disciplines and critical information asset protection;
- Identifying, assessing and managing information security risks; and,
- Conducting Security Threat and Risk Assessments of high profile initiatives.

#### 1.2.1.2 b) Security co-ordination within a ministry

Each ministry should establish a Ministry Information Security Committee to co-ordinate its security activities by:

- Determining the information security priorities and requirements of the ministry;
- Ensuring standards, procedures and processes are developed, documented and implemented to support day-to-day information security activities in compliance with policy;
- Promoting information security awareness and education;
- Communicating priorities and issues to the cross-government information security forum; and,
- Ensuring the Information Incident Management Process is followed for all suspected or actual information incidents.

**Recommended Tests:**

**Note:** 1.2.1.2 is not reported on as part of the annual information security review.

- Demonstrate an active cross-government information security forum.
- Demonstrate ministry information security committee activities.

### 1.2.1.3 Information security responsibilities must be documented.

<table>
<thead>
<tr>
<th>a) Information security responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) Information Owners</td>
</tr>
<tr>
<td>c) Information Custodians</td>
</tr>
<tr>
<td>d) Ministry Chief Information Officer</td>
</tr>
<tr>
<td>e) Ministry Information Security Officer</td>
</tr>
<tr>
<td>f) Chief Records Officer</td>
</tr>
<tr>
<td>g) Supervisors</td>
</tr>
<tr>
<td>h) Employees</td>
</tr>
</tbody>
</table>

**Purpose:** To define security roles and responsibilities for information and information systems.

#### 1.2.1.3 a) Information security responsibilities

Responsibility for security throughout government includes defining:
• The Information Owner and Information Custodian responsible for information and information systems;
• The assets and security processes; and,
• Authorization levels for access.

1.2.1.3 b) Information Owners
Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

Information Owners have the responsibility and decision making authority for information throughout its life-cycle, including creating, classifying, restricting, regulating and administering its use or disclosure and will:
• Determine business requirements including information security needs;
• Ensure Security Threat and Risk Assessments are performed regularly to identify and minimize the risks to information and information systems they own;
• Ensure information and information systems are protected commensurate with their information classification and value;
• Define security requirements during the planning stage of any new or significantly changed information system;
• Determine authorization requirements for access to information and information systems;
• Approve and regularly review access privileges for each employee or set of employees;
• Document information exchange agreements;
• Develop service level agreements for information systems under their custody or control;
• Implement processes to ensure employees are aware of their security responsibilities;
• Monitor that employees are fulfilling their security responsibilities;
• Be involved with security reviews and/or audits; and,
• Follow the Information Incident Management Process for all suspected or actual information incidents.

1.2.1.3 c) Information Custodians
Information Custodians maintain or administer information assets on behalf of the Information Owners by:
• Providing and managing security for the information asset throughout its life-cycle;
• Maintaining and operating the technical infrastructure that information and information systems reside on;
• Maintaining and operating the security infrastructure protecting information and information systems;
• Ensuring that the identified security controls are implemented throughout the supply chain;
• Identifying and minimizing risks to information and information systems by regularly assessing the effectiveness of the security controls of the infrastructure or service, and threats to the information and information systems; and,
• Follow the Information Incident Management Process for all suspected or actual information incidents.
1.2.1.3 d) Ministry Chief Information Officer

The responsibilities of the Ministry Chief Information Officer (MCIO) are defined in the Core Policy and Procedures Manual, Chapter 12 – Information Management and Information Technology Management. In addition to these responsibilities, the Ministry Chief Information Officer is responsible for:

- Being the single point of contact for information incidents within their ministry;
- Being a member of cross-ministry IM/IT forums;
- Ensuring that the Information Incident Management Process is followed for all actual or suspected information incidents;
- Ensuring information security reviews and audits are supported by the ministry; and,
- Ensuring that the ministry business risks do not increase corporate risk.

1.2.1.3 e) Ministry Information Security Officer

The Ministry Information Security Officer (MISO) is responsible for:

- Knowing the information security policy and standard requirements and communicating them within their ministries;
- Assisting business areas to understand and be in compliance with information security policies and standards;
- Ensuring that procedures to support day-to-day security activities are documented in compliance with the Information Security Standard;
- Co-ordinating information security awareness and education activities and resources;
- Providing up-to-date information on issues related to information security;
- Facilitating business areas with conducting Security Threat and Risk Assessments;
- Ensuring that each information system has a current System Security Plan;
- Providing advice on security requirements for information systems development or enhancements;
- Co-ordinating ministry information security initiatives with cross-government information security initiatives;
- Providing advice on emerging information security standards relating to ministry specific lines of business; and,
- Raising ministry security issues to the cross-government information security forum.

1.2.1.3 f) Chief Records Officer

The Chief Records Officer (CRO) is responsible for Information Management (IM) in the Government of British Columbia and leads the Corporate Information and Records Management Office (CIRMO). CIRMO ensures that the mandate of the CRO is carried out.

1.2.1.3 g) Supervisors

Supervisors are employees with direct reports, and are responsible for:

- Knowing and communicating information security policies and standards to employees;
- Ensuring that employees are informed of their responsibilities regarding information security and privacy;
- Ensuring that employees receive the necessary training on information security and have opportunities to participate in security awareness activities; and,
- Ensuring that employee access to government information resources is based on need-to-know and least privilege principles.
Supervisors must review employee access rights to information resources on a regular basis and particularly whenever there is a new employee or a change in employee roles and responsibilities.

1.2.1.3 h) Employees
Employees are responsible for knowing, understanding and complying with information security policies and standards. They should seek guidance from their Supervisors or Ministry Information Security Officers regarding questions on information security policies or any other security concerns.

Recommended Tests:
Note: 1.2.1.3 is reported as part of the annual information security review.
- Demonstrate delegated authority from the Information Owner to Information Custodians.
- Demonstrate the MCIO, MISO and delegated Supervisors are briefed and understand their responsibilities.
- Demonstrate that security responsibilities are communicated to employees.

1.2.1.4 Security roles and responsibilities for employees must be documented.

a) Security roles and responsibilities
b) Communication of security roles and responsibilities

Purpose: To ensure employees are informed of their information security roles and responsibilities.

1.2.1.4 a) Security roles and responsibilities
Employees must be aware of their information security roles and responsibilities. Information Owners and Information Custodians must:
- Document information security roles and responsibilities for employees in job descriptions, standing offers, contracts, and information use agreements where relevant; and,
- Review and update information security roles and responsibilities when conducting staffing or contracting activities.

1.2.1.4 b) Communication of security roles and responsibilities
Supervisors must ensure employees are informed of their security roles and responsibilities by establishing processes for communicating security roles and responsibilities to protect information assets.

Recommended Tests:
Note: 1.2.1.4 is not reported on as part of the annual information security review.
- Demonstrate security roles and responsibilities are documented.
- Demonstrate security roles and responsibilities are reviewed on a regular basis.
- Demonstrate a formal process for informing employees of their security roles and responsibilities.

1.2.1.5 Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of information systems.

a) Segregation of duties
b) Critical or sensitive information systems

Purpose: To reduce risk of loss, fraud, error and unauthorized changes to information.
1.2.1.5 a) Segregation of duties
Information Owners and Information Custodians must reduce the risk of disruption of information systems by:
- Requiring complete and accurate documentation for every information system;
- Requiring that no single individual has access to all operational functions of an information system (e.g., operating system administrators must not also have application administrator privileges);
- Rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight on key systems;
- Automating functions to reduce the reliance on human intervention for information systems;
- Requiring that individuals authorized to conduct sensitive operations do not audit the same operations;
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action; and,
- Implementing security controls to minimize opportunities for collusion.

1.2.1.5 b) Critical or sensitive information systems
Where supported by a Security Threat and Risk Assessment or other formal assessment, Information Owners and Information Custodians must employ two-person access control to preserve the integrity of the information system.

**Recommended Tests:**

*Note: 1.2.1.5 is reported on as part of the annual information security review.*
- Demonstrate access analysis that confirms privileged user controls are limited to job responsibilities.
- Demonstrate job rotation to avoid sole control on key systems.
- Demonstrate no one person is responsible for the operation and audit of critical systems.
- Demonstrate financial risk control reviews and/or independent audits that demonstrate segregation of duties has been done adequately.

1.2.1.6 Appropriate contacts shall be maintained with local law enforcement authorities, emergency support employees.

**a) Contact with authorities**

*Purpose: To facilitate timely response from and co-ordination with outside authorities during information security incidents or investigations.*

1.2.1.6 a) Contact with authorities
The Chief Information Security Officer must ensure that outside authorities, emergency support employees can be contacted by:
- Maintaining and distributing as appropriate, a list of internal and external organizations and service providers; and,
- Documenting emergency and non-emergency procedures for contacting authorities as required during information security incidents or investigations.
Recommended Tests:

1.2.1.6 Recommended Tests:

Note: 1.2.1.6 is reported on as part of the annual information security review.

- Demonstrate emergency and non-emergency procedures for contacting external authorities that may be required during information security incidents or investigations.
- Demonstrate a process for maintaining the accuracy of contact lists.
- Demonstrate that the contact lists are reviewed and updated at a minimum annually (e.g., part of the Business Continuity Program review).

1.2.1.7 (Para.1)

Appropriate contacts shall be maintained with specialist security forums and professional associations.

a) Participation in security forums and professional associations

Purpose: To promote and further employee knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities.

1.2.1.7 a) Participation in security forums and professional associations

Information security specialists must maintain their knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities by:

- Participating in information exchange forums regarding best practices, industry standards development, new technologies, threats, vulnerabilities, early notice of potential attacks, and advisories;
- Maintaining and improving knowledge regarding information security best practices; and,
- Creating a support network of other security specialists.

The Chief Information Security Officer must promote professional certification and membership in professional associations for information security specialists throughout government.

Recommended Tests:

Note: 1.2.1.7 is reported on as part of the annual information security review.

- Demonstrate that employees with information security responsibilities maintain professional associations.
- Demonstrate employees with security responsibilities have appropriate certification by a recognized security forum.
- Demonstrate employees with security responsibilities attend security meetings, security conferences and information sessions.

1.2.1.8 (Para.1)

Where projects involve information or information technology assets the information security must be addressed in project management.

a) Information security in project management

Purpose: To ensure that information security risks are identified and addressed throughout the project life-cycle.

1.2.1.8 a) Information security in project management

Information Owners and Information Custodians must integrate information security into every phase of the organization’s project management method(s) to ensure that information security risks are
identified early and addressed as part of the entire project. The project management methods in use should require that:

- Information security objectives are included in project objectives;
- An information Security Threat and Risk Assessment is conducted at an early stage of the project to identify necessary controls; and,
- Information security is part of all phases of the applied project methodology.

Information security implications should be reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in project management methods.

**Recommended Tests:**

*Note: 1.2.1.8 is reported on as part of the annual information security review.*

- Demonstrate that information security objectives are identified in project objectives.
- Demonstrate that information Security Threat and Risk Assessments are conducted at an early stage of a project to identify required security controls.
- Demonstrate that information security is applied during all phases of a project and are reviewed regularly.
- Demonstrate security roles are defined in the project management methodology.

### 1.2.1.9 Establishment of new information systems and processing facilities requires formal management authorization.

- **a) Approval for information processing facilities**
- **b) Approval for information systems**
- **c) Acquisition of hardware, firmware and software**
- **d) Use of non-government hardware**

**Purpose:** To ensure the secure operation of new or significantly modified information systems and information processing facilities using a formal review and approval process.

### 1.2.1.9 a) Approval for information processing facilities

Prior to constructing any new information processing facilities, Information Owners and Information Custodians must:

- Conduct a Security Threat and Risk Assessment;
- Conduct a Privacy Impact Assessment;
- Address security requirements in the construction of the facility;
- Conduct a risk and controls review to determine if controls are adequate to mitigate business risks prior to implementation of the information processing facility; and,
- Obtain advice from the Office of the Government Chief Information Officer to ensure adherence to relevant policies, procedures, standards and guidelines.

### 1.2.1.9 b) Approval for information systems

Information Owners and Information Custodians of a new or significantly modified information system must:

- Conduct a Security Threat and Risk Assessment;
- Conduct a Privacy Impact Assessment;
- Address security requirements in the development of the system;
• Conduct a risk and controls review to determine if controls are adequate to mitigate business risks prior to implementation of the information system;
• Ensure new and significantly changed information systems undergo certification and accreditation; and,
• Obtain approval from the Office of the Government Chief Information Officer to ensure adherence to relevant Core Policies and Procedures, including the Information Security Policy, and the Information Security Standard.

1.2.1.9 c) Acquisition of hardware, firmware and software
Prior to acquisition of new hardware, firmware or software, Information Owners and Information Custodians must:
• Ensure new hardware, firmware and software conform to government standards;
• Evaluate compatibility with existing information systems hardware, firmware and software;
• Consider the reliability of the product as part of the procurement selection process; and,
• Evaluate the need for any additional security measures and the impact on existing security processes.

Information Owners and Information Custodians can consult with the Office of the Government Chief Information Officer for assistance with decision-making on the acquisition of hardware, firmware and software.

1.2.1.9 d) Use of non-government hardware
When using non-government hardware, employees must follow the Appropriate Use Policy and meet the requirements for collection, access, use, disclosure, storage and disposal of government information. Employees must not store government information on non-government hardware, unless there is an extenuating circumstance, in accordance with the Appropriate Use Policy. The process must address, at a minimum, requirements for information security, privacy, data ownership, and support.

Recommended Tests:
Note: 1.2.1.9 is not reported on as part of the annual information security review.
• Demonstrate a formal review and approval process exists for establishing new or significantly modified information systems and processing facilities.
• Demonstrate an approval process for non-government hardware.
2  Mobile computing and Teleworking

Please see the Mobile Computing Security Standard (at: IM/IT Standards).

Please see the Teleworking Security Standard (at: IM/IT Standards).

3  Human Resource Security

Please see the Human Resource Security Standard (at: IM/IT Standards).

4  Asset Management

Please see the Asset Management Security Standard (at: IM/IT Standards).

5  Access Control

Please see the Access Control Security Standard (at: IM/IT Standards).

6  Cryptography

Please see the Cryptographic Controls Security Standard (at: IM/IT Standards).

7  Physical and Environmental Security

Please see the Physical and Environmental Security Standard (at: IM/IT Standards).
8 Operations Security

Please see the Operations Security Standard (at: IM/IT Standards).

9 Communications Security

Please see the Communications Security Standard (at: IM/IT Standards).

10 System Acquisition, Development and Maintenance

Please see the System Acquisition, Development and Maintenance Security Standard (at: IM/IT Standards).

11 Supplier Relationships (and Cloud Computing)


12 Information Security Incident Management

Please see the Information Security Incident Management Security Standard (at: IM/IT Standards).
13 Information Security Aspects of Business Continuity Management


14 Compliance

Please see the Compliance Security Standard (at: IM/IT Standards).
Appendix A – Glossary

Accreditation – the final approval to authorize operation of an information system and to explicitly accept the risk to Ministry operations (including mission, functions, image, or reputation), assets, or individuals, based on the implementation of an agreed upon set of security controls.

Ad hoc telework – occasional telework that may not have a formal agreement in place. (See: telework)

Application (business 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.

Assets – for the purposes of information security policy, information in all forms and media, networks, hardware, software and application systems.

Audit – is an examination of the facts to render an opinion and would include testing evidence to support the opinion.

Audit logs – includes all types of event logs including (but not limited to) security, audit, application, access and network across all operating system platforms.

Authentication – the verification of the identity of a person or process.

Availability – information or information systems being accessible and usable on demand to support business functions.

Business Continuity Plan (BCP) – the procedures and information necessary for the timely recovery of essential services, programs and operations, within a predefined timeframe. The BCP includes the recovery following an emergency or a disaster that interrupts an operation or affects service or program delivery.

Business information systems – internal administrative and productivity information systems that support the organization such as e-mail, calendars and financial systems.

Capacity management – the process of determining the system capacity needed to deliver specific performance levels through quantification and analysis of current and projected workload.

Certification – See: security certification

Chief Information Security Officer – responsible for protecting the confidentiality, integrity and availability of government information.

Cloud Computing – Cloud computing is a term used to describe on-demand resource pooling, rapid elasticity and measured services with broad network access (e.g., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)) (based on the NIST definition).

Commercial-off-the-shelf (COTS) – commercially available products that can be purchased and integrated with little or no customization.

Compliance checking – in the context of the Information Security Standard, includes: an audit; risk and controls review; security review; and monitoring of an information system.

Confidentiality – information is not made available or disclosed to unauthorized individuals, entities or processes.

Control – (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure. Where the information in a record directly relates to more than one public body, more than one public body may have control of the record. (See: the Freedom of Information and Protection of Privacy Policy and Procedures Manual for further information.)

Control balances – computational aids for data verification (e.g., records counts, row and column counts, sub-totals, etc.).

Critical – processes that, should they not be performed, could lead to loss of life ("safety"), personal hardship to citizens, major damage to the environment, or significant loss in revenue and/or assets.

Cryptographic Keys – a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of data into encrypted data and the transformation of encrypted data into data during decryption. The cryptographic algorithm ensures that only someone with knowledge of the key can reproduce or reverse the transformation of data.

Cryptography – the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.
**Custody** – (of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.

**Data** – an individual fact (datum) or multiple facts (data), or a value, or a set of values, 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.

**Diagnostic Ports** – ports, services and systems used for diagnostic, maintenance and monitoring activities for managing information system performance, function or capacity. Examples include: physical network switch diagnostic ports, logical management services such as SNMP and modems for remote maintenance.

**Digital signing** – refers to an attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users’ private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the 'digitally signed' document) that can only be decrypted by applying the user’s public key. (Also digitally signing, digital signature)

**Disaster Recovery Plan** (DRP) – the procedures and information necessary to recover critical IT functions from any event that may interrupt an operation or affect service or program delivery, within the timeframes determined in the Business Impact Assessment. The DRP is part of a ministry's overall business continuity plan (Business Continuity Plan or BCP).

**Disposition** – the actions taken regarding information that is no longer needed to support on-going administrative and operational activities in accordance with an approved Records Management Schedule. Directions may include destroy, transfer to the government archives, transfer to inactive records storage space, or retain permanently within unit.

**Electronic agent** – a computer program, or other electronic means, used to initiate an activity or to respond to electronic information, records or activities in whole or in part without review by an individual at the time of the response or activity.

**Electronic commerce** – the exchange of information between government and internal and external stakeholders independently of either participant’s computer system (e.g., electronically accessing forms, obtaining payments, sending invoices, receiving tax returns, placing orders and receiving transaction acknowledgements).

**Electronic messages** – includes all forms of electronic messaging such as e-mail, voice mail, instant messaging, etc.

**Employee** – an individual working for the Government of British Columbia, including service providers or volunteers.

**Equipment** – See: Hardware

**Essential services** - Essential business processes are those processes defined as critical and business-priority and essential to delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each essential business process.

**External Party** – a person external to “government” as defined within the Financial Administration Act.

**Fault** – an error or failure in either software or hardware.

**Firmware** - programming that is inserted into programmable read-only memory becoming a permanent part of a computing device.

**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.

**Government network** – See: Network Infrastructure.

**Government records** – See: Government information.

**Hardware** – includes (but not limited to) servers, desktop computers, printers, scanners, fax machines, photocopiers, multi-function devices, routers, communications and mobile equipment, cell phones, mobile devices and removable media.

**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. (See: Government Information).

**Information asset** – includes all data, information and intellectual property.

**Information classification label** – a designation indicating the information classification (e.g., “Public”, “Standard”, “High”).
**Information Custodians** – maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. In contrast, information custody means having physical possession of information without necessarily having responsibility for the information.

**Information Labelling** – affixing a physical or electronic label identifying the security category of a document, file or records series in order to alert those who handle it that it requires protection at the applicable level.

**Information Owners** – have the responsibility and decision-making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure. Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

**Information Processing Facilities** – the physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

**Information Security** – preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

**Information Security Activities** – management and technology programs to protect government information assets.

**Information Security Architecture** – a strategy that consists of layers of policy, standards and procedures and the way they are linked to create an environment in which security controls can be easily established.

**Information Security Classification** – a system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability. (Also classification, information classification, security classification)

**Information Security Event** – an identified occurrence of a system or service state indicating a possible breach of information security or failure of safeguards, or a previously unknown situation that may be security relevant.

**Information Security Incident** – 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.

**Information Security Policy** – with the introduction of version 4 of the Information Security Policy, the document is considerably shorter, less technical, and intended to provide direction with regards to government’s information security practices. It is for all government staff, particularly those with responsibility and decision-making authority to manage government information and information technology.

**Information Security Program** – See: Information Security Standard 1.2.1.1

**Information System** – any equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

**Information System Security Classification** – a system of designating security categories for information systems based on the information security categories of information processed by the information system.


**Information Technology Asset** – includes owned and leased technology hardware (i.e. physical items), owned or licensed software and related or supporting services.

**Information 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 Type** – information classes or groupings based on function, usage, attributes or other commonality (e.g., employees records, invoices, or system documentation are information types). Address, name, or birth date are examples of discrete data elements.
**Integrity**—the characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

**Intellectual property**—intellectual property refers to the category of intangible (non-physical) property consisting primarily of rights related to copyrighted materials, trademark, patent and industrial design. Intellectual property rights are associated with a wide range of products of the human intellect, such as training manuals, publications, map products, videos and computer software. It is important to keep clear the distinction between the items that give rise to intellectual property, such as the manuals and software, and the intellectual property itself, which is the set of rights arising from the creation and development of the items. Simply put, the items are the copies of a particular book, whereas the intellectual property is the copyright in that book.

**Key Management**—the processes for the generation, exchange, storage, safeguarding, use, vetting and replacement of cryptographic keys.

**Least Privilege**—a security principle requiring that each subject in a system be granted the most restrictive set of privileges (or 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.

**Malicious code**—malicious code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources. Types of malicious code can include viruses, worms, Trojans, spyware and denial of service attacks.

**Media**—Material that information is written to and stored on. See: Records.

**Message integrity**—the assurance of unaltered transmission and receipt of a message from the sender to the intended recipient to maintain the completeness, accuracy and validity of the information contained in the message.

**Ministry Information Security Officer**—responsible for co-ordinating the ministry security program for protecting the confidentiality, integrity and availability of government information.

**Mobile code**—multiplatform computer code that can be downloaded or transmitted across a network that runs automatically on a computer with little or no user interaction. Software technologies such as, for example, Java, JavaScript, VBScript, ActiveX, provide the mechanisms for the production and use of mobile code.

**Mobile computing service**—a service that provides access to government systems from Mobile Computing Devices. Distinct from Remote Access Services in that the mobile computing service provides product-specific access to limited applications rather than full standard network access (e.g., BlackBerry Enterprise Server service).

**Mobile devices**—portable self-contained electronic devices, including laptops, tablets, smartphones, cell phones, digital cameras, etc.

**Monitoring**—a regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards.

**Multi factor authentication**—this is combining two or more authentication techniques together to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: Secret—something the person knows; Token—something the person has; Biometric—something the person is.

**Need to Know principle**—a privacy 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.

**Network Address Spoofing**—forging or faking source network addresses with the intent to obscure, hide or impersonate the actual source device.

**Network infrastructure**—the equipment, information systems and cabling systems used to establish a communication network between Information Systems. Includes routers, switches, hubs, firewalls, transmitters, fibre optic cable and copper cable.

**Network management information**—the information used to manage network infrastructure, including traffic statistics, counters and logs.

**Network pathways and routes**—the physical and logical pathways that comprise the connections within the network infrastructure.

**Network security boundary**—the logical or physical boundary between networks of differing security protection requirements. Network access control devices demark the network security boundaries.

**Network security zone**—a logical entity containing one or more types of services and entities of similar security requirements and risk levels.
Network segregation – the separation of groups of users, information systems and services with similar business functions by control of network traffic flow (e.g., by use of security gateways, physically separate networks or access controls).

Network service agreement – The contract or agreement between a service provider and a service consumer which defines the services to be delivered and the terms and conditions of delivery.

Network service provider – a provider of network services to government which may be internal or external to government.

Non-repudiation - the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Non-retrievable – unable to recover the data from any media in any form.

Outside authorities – include law enforcement, fire departments, other emergency response authorities, utilities and telecommunications providers.

Password management system – An automated process which enforces password rules (e.g., IDIR or RACF).

Portable storage devices – portable (or removable) device that is primarily designed to store electronic information (e.g., an external hard drive or a USB flash drive).

Positional user identifier (userid) – is a unique system userid assigned to a persistent function or job in circumstances where the employees filling the job are transitional. Positional userids are issued to a Supervisor who is accountable for the day to day management and assignment of the userid to individuals (e.g., a positional userid could be used if a receptionist position was temporarily filled by short term employees from an employment agency). In these limited circumstances use of positional userids can avoid creating new userids for short term employees.

Privacy – the right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in records.

Privacy Impact Assessment – an assessment that is conducted to determine if a new enactment, system, project or program meets the requirement of Part 3 of the Freedom of Information and Protection of Privacy Act.

Privileged operations – permissions which allow the user to alter access rights and structures of information systems and/or services.

Privileged users – users with permissions to alter access rights and structures of information systems. This includes (but is not limited to) system administrators, network administrators, database administrators, security administrators, web site administrators, system operators and network operators.

Privileges – See: privileged operations.

Reception Zone – an area where the initial contact between the public and the ministry occurs, where services are provided, information exchanged and access to restricted zones is controlled.

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

Remote access – the act of using a remote access service to connect to the government network or government systems.

Remote access service – a service that provides network access to the government network or government systems from a remote location (e.g., the government VPN service).

Requirements phase – one component of the System Development Life Cycle. Functional user requirements are formally defined and delineate the requirements in terms of data, system performance, security and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. All requirements need to be measurable, testable and related to the business need or opportunity.

Restricted Access Operations Zone – a controlled area where access is limited to persons who work there and to escorted visitors. It is usually a standard working area and offices.

Restricted Access Security Zone – a strictly controlled area where access is limited to authorized persons and to properly escorted visitors.

Risk – Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

Risk and controls review – an independent and objective assessment of an information system to determine whether the business/system framework has adequate controls to mitigate business, financial, security and general privacy risks.
Screening – to verify facts about individuals related to their identity, professional credentials, previous employment, education and skills.

Secured Path – a network path that has been protected from eavesdropping, intrusion and data tampering.

Security categories – inform employees how to handle records in order to protect them and determine requirements for marking, storage, transport, transmittal, disposal and destruction.

Security certification – a comprehensive assessment of the management, operational and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security infrastructure – the complete set of information security-related systems, policies, standards, guidelines, procedures, resources and physical implementations of information security administration.

Security Management Systems – systems that collect, store and manage configuration and operational information about network devices. Includes configuration management databases and log management systems.

Security posture – the security status of the technical infrastructure and information systems to known vulnerabilities and attacks.

Security review – an independent review with the scope focused on the security framework over the business processes, application and operating environment. Reviews are distinguishable from audits in that the scope of a review is less than that of an audit and therefore the level of assurance provided is lower.

Security Threat and Risk Assessment – a component of a risk analysis specifically aimed at identifying security exposures. Security Threat Risk Assessments, commonly known as STRAs include, but are not limited to, security assessments, vulnerability testing, penetration testing, audit reviews.

Security weakness – a weakness in an application, procedure or process that may result in a security incident.

Security zone – See: reception zone, restricted access operations zone, restricted access security zone.

Service provider – means a person retained under contract to perform service for the Government of British Columbia.

Software – includes (but not limited to) application and system software, development tools, utilities.

Status Accounting – a comparison of configuration data stored in a configuration database to actual device configuration. Used to ensure that recorded configuration data matches actual device configuration.

Supervisor – is accountable for human resource leadership and management within their business unit.

System Security Plan – repository to document security information and controls (management, operational and technical) regarding an application system.

System Utility Programs – Tools that when misused can subvert system, access and application controls (e.g., network sniffers, password crackers, port scanners, root kits and vulnerability assessment scanners).

Systems documentation – detailed information about a system's design specifications, its internal workings, and its functionality including schematics, architectures, data structures, procedures and authorization processes.

Systems privileges – permissions which allow the user to alter access rights and structures of information systems.

Telework – a working arrangement where employees work away from their official workplace for a portion of their regular work week (BC Public Service Agency, Flexible Work Options). (See: ad hoc telework)

Third party – includes external party and includes a person outside the direct reporting structure of the Information Owner or Information Custodian (e.g., an individual, a business or organization, employees from another branch of government, or another level of government).

Threat – in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, disposal, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin. (See: vulnerability and information security event).

Trusted path – See: secured path

Two-person access control – a system of requiring the presence of two authorized persons to perform an action, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. For example, a locked cabinet or safe which has two locks requiring action by two persons, each with a unique key or code and which requires the presence of two persons to access or open.

Uninterruptible power supply – a backup power source for computers and computer networks to insure on-going operation in the event of a power failure.
User – all persons authorized to access the government’s electronic services and information systems, including employees and contractors.

User identifier – is the unique personal identifier that is authorized to access the government's computer and information systems.

Vulnerability – in the security context, a weakness in security procedures, processes, or controls that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Wireless Local Area Network – a Local Area Network that uses wireless transmission media, such as 802.11a/b/g/n or WiMax.

Zone – See: reception zone, restricted access operations zone, restricted access security zone.
Appendix B – List of commonly used references

( Indicates a BC Government login is required to access the site.)

Appropriate Use of Government Information and Information Technology Resources

- Appropriate Use Policy –
  https://www2.gov.bc.ca/gov/content?id=33A6DE0643E54676B21033E5DA8E03CF
- Information and Communications Technology (ICT) Agreement -
  http://www2.gov.bc.ca/assets/gov/careers/forms-tools/all-employees/information_communication_technology_agreement.pdf

Asset Disposal Standard – IT Security


- Information Management Act -
  http://www.bclaws.ca/civix/document/id/complete/statreg/15027

BC Public Service Agency

- Security Screening - http://www2.gov.bc.ca/myhr/content_hub.page?ContentID=ea3328ba-7d38-5d2c-2818-f4fd2a64db33
- The Learning Centre -
  https://www2.gov.bc.ca/gov/content?id=E5BEF2195D9C436E893D398F04C0024E

Core Policy and Procedures Manual (CPPM)

- Chapter 6 – Procurement
- Chapter 8 – Asset Management
- Chapter 12 – Information Management and Information Technology Management
- Chapter 14 – Risk Management
- Chapter 15 – Security
- Chapter 16 – Business Continuity Management
- Chapter 20 – Loss Management

Corporate Information and Records Management Office – Freedom of Information
http://www2.gov.bc.ca/gov/content/governments/about-the-bc-government/open-government/open-information/freedom-of-information

Corporate Information and Records Management Office – Privacy
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy

- Personal Information Protection Act (PIPA) - http://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information
- Privacy Impact Assessment Process (PIA) - http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments
- Privacy and Information Sharing training - http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/training

Corporate Information and Records Management Office – Records Managements
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management

Corporate Information Risk Reporting
https://intranet.gov.bc.ca/intranet/content?id=061697A1F2294C8C832A91D73564F036

Critical Systems Standard

Critical Systems Guidelines

Cryptographic Standards for Information Protection

Exemptions from an Information Security Policy or an IM/IT or Architecture Standard
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/exemptions

Flexible Workplace and Information Security – includes telework agreements
http://www2.gov.bc.ca/myhr/article.page?ContentID=b241b2be-d1cf-3106-72d8-4ef4d189d38a

General Service Agreement and Schedule G Information
http://www2.gov.bc.ca/gov/content/governments/services-for-government/bc-bid-resources/templates-and-tools/service-contract-templates/general-service-agreement-information
Information Incident Management Process (IIMP)
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents
- Information Incident Management Process - policy
- Process for Responding to Privacy Breaches - read in conjunction with the IIMP
- Information Incident Checklist - provides high level guidance for responding

Information Management/Information Technology (IM/IT) Standards
- http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards (main page)
- http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard (Find a Standard)

Information Security Awareness Resources (Information Security Branch)
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness

Information Security Branch
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security

Information Security Classification Framework
https://www2.gov.bc.ca/gov/content?id=7430B7CCF0FE459F93A554E72DF21503

Information Security Standards and Guidelines

Intellectual Property Services
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/intellectual-property

Oath of Employment for BC Public Service Employees
https://www2.gov.bc.ca/gov/content/careers-myhr/all-employees/new-employees/when-you-start/first-three-months/oath

Office of the Government Chief Information Officer
http://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/office-of-the-chief-information-officer
- OCIO Enterprises Services Division intranet site - https://intranet.gov.bc.ca/thehub/ocio/ocio-enterprise-services/

Office of the Chief Information Officer (OCIO) Helpdesk - Client Resource Centre
https://ssbc-client.gov.bc.ca/
• Service Bulletins - https://ssbc-client.gov.bc.ca/servicenews/default.htm
• A to Z Services Index - https://ssbc-client.gov.bc.ca/services/Index_AZ.htm

Provincial Identity Management Program (IDIM)
https://intranet.gov.bc.ca/thehub/ocio/technology-solutions/provincial-idim-program

Government Chief Risk Office
https://www2.gov.bc.ca/gov/content?id=FEC0B15383054F44899979BE6F67CA837
  • General Incident or Loss Report (GILR) process and form - http://gilr.gov.bc.ca/


Security Threat and Risk Assessment (STRA)
  • STRA information - https://www2.gov.bc.ca/gov/content?id=7175C19B66564EA3A343AB8B668BEFC2

Standards of Conduct for BC Public Service Employees
  • MyHR site - http://www2.gov.bc.ca/myhr/article_page?ContentID=45bf7662-adf9-8a5f-74f1-657fedd69edf&PageNumber=1

Working Outside the Workplace Policy
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/working-outside-workplace