OCIO | Office of the Chief Information Officer

Information Security Policy

Version 3.0
July 2016

BRITISH COLUMBIA

Table of Contents

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 Policy 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 Policy 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 Policy 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 the Information Security Policy.

II Scope

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

Exemptions from an Information Security Policy or 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 Revisions from ISP 2.2 (2012) to ISP 3.0 (2016)

Version 3.0 of the Information Security Policy represents some significant updates from Version 2.2, in both the organization of the document and specific policy changes driven by a variety of factors.

Policy Content Changes

"Policy is intended to enable things to happen by giving people the direction they need to do their work properly and consistently. Information security policies document appropriate behaviour and clearly describe what must be done, and what is or is not allowed." (from Security 101 Guidebook)

Information Management, Technology and Security are in a constant state of growth and fluctuation. Government must respond appropriately to ensure that the information security foundation supports these changes and provides employees with the tools necessary to perform their responsibilities. Version 3.0 contains a number of such updates:

- new or revised policies and references to standards in support mobile working and teleworking;
- the protection of test data, including the use of production data for testing;
- the appropriate use of information resources;
- the payment card industry data security standard; and
- cloud computing.

The new *Information Management Act* (Bill 5) has replaced the *Document Disposal Act* as government's primary records management law and sets the foundation for government's transition towards digital information management.

Organization of the document

References – a master list of references is included at the front of the document that ISP users can refer to *(Section V, p.7)*. This eliminates the need of overcrowding the policies with repeating reference sections. The ISP document focusses on the policy content and a hyperlink change can be done only once.

Numbering - Anyone familiar with the Information Security Policy will immediately see that there are more chapters and the ordering of the individual policies has changed in many instances. Feedback received from Ministry Information Security Officers and other ISP users was that the numbering of ISP policies was different than the policies in the ISO Standard 27002:2013. In response to this request, Version 3.0 has been re-ordered as needed to match the ISO Standard table of contents. A comparison document between ISP v2.2 and the new ISP v3.0 highlights the high-level changes and is available together with the policy.

Annual Information Security Review – As required under Chapter 12 of the CPPM, the Information Security Branch works with ministries on annually reviewing their compliance with the Information Security Policy using the iSMART tool and the ISO Standard. Throughout Version 3.0 of the ISP, the policies are following by the statement *"ISP # is reported on as part of the annual information security review as CO.#"*. CO refers to the *Control Objectives* statements in iSMART. This addition is provided to facilitate ease of use.

Metrics and Enforcement statements – In Version 2.2, *Metrics and Enforcement* statements were suggested for each policy as a tool for users to self-evaluate the application of the policy. In Version 3.0, the term *Recommended Tests* is used instead, to better reflect the intent.

IV Terms and definitions

There are some word pairs used in the Information Security Policy that users have found cause confusion and require clarification. Because they do apply to the ISP 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 "**mus**t" 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 policy requirement does not apply. Where for certain reasons a Ministry or a program area cannot comply with a specific policy or 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

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

Appropriate Use of Government Information and Information Technology Resources

- CPPM 12.3.1 - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1231
- Appropriate Use Policy - http://www.cio.gov.bc.ca/cio/appropriate_use/index.page
- 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
http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/it_asset_disposal_standard.pdf

- Disposal Handbook - http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/buy-goods-services-and-construction/reference-resources/disposal_handbook.pdf
- 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 - http://www2.gov.bc.ca/myhr/article.page?ContentID=6a97ec64-ab44-da75-3994-6bdcd988efc1
- Human Resource Policies - http://www2.gov.bc.ca/gov/content/careers-myhr/managers-supervisors/employee-labour-relations/conditions-agreements/policy

Core Policy and Procedures Manual (CPPM) – Table of Contents
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm#toc2

- Chapter 6 – Procurement - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/06_Procurement.htm
- Chapter 8 – Asset Management - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/08_Assets.htm
- Chapter 12 – Information Management and Information Technology Management - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm
- Chapter 14 – Risk Management - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/14_Risk_Mgmt.htm
- Chapter 15 – Security - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/15_Security.htm
- Chapter 16 – Business Continuity Management - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/16_Business_Continuity_Mgmt.htm
- Chapter 20 – Loss Management - http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/20_Loss_Mgmt.htm

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

- Freedom of Information and Protection of Privacy Act - http://www.bclaws.ca/Recon/document/ID/freeside/96165_00
- 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 Management and Accountability Policy - http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/policies-guidelines/privacy-management-accountability-policy.pdf
- 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/thehub/ocio/technology-solutions/information-security-branch/vulnerability-and-risk-management/corporate-information-risk-reporting

Critical Systems Standard
http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/critical_systems_standard.pdf

Critical Systems Guidelines
http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/critical_systems_guidelines_v1-4.pdf

Cryptographic Standards for Information Protection
http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/cryptographic_standards.pdf

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)
- Categories: Appropriate Use, Software Development, Information, Identity, Technology and Security.

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 Tips - articles on Wikilumbia @Work
- Information Security Glossary - on Wikilumbia

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

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

Information Security Standards and Guidelines
https://intranet.gov.bc.ca/thehub/ocio/technology-solutions/information-security-branch/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
http://www2.gov.bc.ca/gov/content/careers-myhr/all-employees/new-employees/first-four-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

- Technology Solutions intranet site - https://intranet.gov.bc.ca/thehub/ocio/technology-solutions

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
- Remote Access Services - https://ssbc-client.gov.bc.ca/services/RemoteAccess/overview.htm

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

Risk Management Branch and Government Security Office
http://www.fin.gov.bc.ca/PT/rmb/index.shtml

- General Incident or Loss Report (GILR) process and form - http://gilr.gov.bc.ca/

Security 101 Guidebook – The Basics of Information Security in the Government of British Columbia
http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/information-security-awareness/security101_basics_info_security_guidebook_jan2014_final.pdf

Security Threat and Risk Assessment Standard (STRA)

- Standard - http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/security_threat_and_risk_assessment_standard.pdf
- STRA process - https://intranet.gov.bc.ca/thehub/ocio/technology-solutions/information-security-branch/vulnerability-and-risk-management/security-threat-risk-assessment

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
- PDF Brochure – Standards of Conduct
  http://www2.gov.bc.ca/local/myhr/documents/jobs_hiring/standards_of_conduct_printable_version.pdf

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

- Home Technology Assessment
- Tip Guide: How to Protect Your Home Computer

1 Information Security Policy

The Information Security Policy 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.

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 operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of government 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 additional 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 the baseline established by the Information Security Policy.

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 in individual policies to assist in interpretation and implementation.

Recommended Tests:
Note: ISP 1.1.1 is reported on as part of the annual information security review as CO.1.4.

- 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: ISP 1.1.2 is reported on as part of the annual information security review as CO.1.6.

- Demonstrate that Ministry specific policies have a development, review and approval process.

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.

2.1 Internal organization

2.1.1	**Executive must set direction and provide support for information security.** **a) Executive support** **b) Chief Information Security Officer** **c) Information Security Branch support**

Purpose: ***To establish executive direction on, and commitment to, information security to maintain the confidentiality, integrity and availability of government information.***

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.

2.1.1 b) Chief Information Security Officer

The Chief Information Security Officer (CISO) 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 Policy, 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 Policy;
- 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.

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: ISP 2.1.1 is reported as part of the annual information security review as CO.2.2.

2.1.2	**Implementation of information security activities across government must be co-ordinated by the Office of the Government Chief Information Officer.** **a) Security co-ordination across government** **b) Security co-ordination within a ministry**

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

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.

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: ISP 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.

2.1.3	**Information security responsibilities must be documented.** **a) Information security responsibilities** **b) Information Owners** **c) Information Custodians** **d) Ministry Chief Information Officer** **e) Ministry Information Security Officer** **f) Chief Records Officer** **g) Supervisors** **h) Employees**

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

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.

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.

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.

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.

2.1.3 e) Ministry Information Security Officer

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

- Knowing the Information Security Policy requirements and communicating them within their ministries;
- Assisting business areas to understand and be in compliance with the Information Security Policy;
- Ensuring that standards/procedures to support day-to-day security activities are documented in compliance with the Information Security Policy;
- 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.

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.

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.

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: ISP 2.1.3 is reported as part of the annual information security review as CO.2.4.

- 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.

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.

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.

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: ISP 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.

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.

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.

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: ISP 2.1.5 is reported on as part of the annual information security review as CO.2.6.

- 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.

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.***

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:

Note: ISP 2.1.6 is reported on as part of the annual information security review as CO.2.8.

- 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).

2.1.7 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.***

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: ISP 2.1.7 is reported on as part of the annual information security review as CO.2.10.

- 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.

2.1.8 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.***

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: ISP 2.1.8 is reported on as part of the annual information security review as CO.2.12.

- 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.

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.***

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.

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 and the Information Security Policy.

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 the Information Security Policy, standards and guidelines;
- 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.

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: ISP 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.

2.2 Mobile computing and teleworking

2.2.1	**Appropriate controls must be implemented to mitigate security risks associated with the use of mobile devices.** **a) Information protection paramount** **b) Service-specific risks and practices** **c) Protection of credentials** **d) Protection of network endpoint and physical device** **e) Human factors** **f) Risk assessment factors**

Purpose: ***To protect information stored on mobile devices from loss or unauthorized access.***

2.2.1 a) Information protection paramount
The use of mobile devices such as laptops, tablets or smartphones to access, store, or process information increases the risk of information compromise. Mobile devices are typically small and portable, used in uncontrolled public environments, and easily lost, stolen or damaged.

Information Owners and Information Custodians must ensure that use of mobile devices is managed and controlled. To ensure that sufficient safeguards are implemented to mitigate risks mobile devices must be enrolled in Mobile Device Management Service. Users of mobile devices must protect the information and information technology assets in their custody or control.

2.2.1 b) Service-specific risks and practices
Providers of mobile computing services (such as Technology Services Division) must perform regular risk assessments to identify service-specific risks (e.g., perform or update the risk assessments on an annual basis). Information Owners and Information Custodians must develop, document and maintain policies, standards, practices and guidelines that address these risks, and communicate them to employees.

2.2.1 c) Protection of credentials
User identifiers and user credentials must be protected to reduce the risk of unauthorized access to information and information technology assets. In particular, employees must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places.

2.2.1 d) Protection of network endpoint and physical devices
Mobile devices are typically used to store information or remotely access government networks and services. The policies and procedures governing remote access apply to mobile devices. Where Remote Access services are used, the mobile device must be configured to prevent its use as a conduit between the non-government and government networks (e.g., VPN split tunnelling must be disabled).

Network access to mobile devices from non-government networks must be blocked by implementation of firewall or filtering technologies to protect against attack (e.g., to prevent network attacks against the mobile device).

Mobile devices must be protected against mobile and malicious code. Mobile devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

2.2.1 e) Human factors
Information Owners and Information Custodians must provide employees using mobile devices with security awareness training to ensure that they are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using mobile devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with the Information Incident Management Process.

2.2.1 f) Risk assessment factors
The Security Threat and Risk Assessment must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of mobile devices to remotely access Government networks and systems;

- Data interception;
- Credential theft;
- Unauthorized device use;
- Device disposal;
- Information disposal;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Information classification and sensitivity levels must be considered in the risk assessment. Storage of government information on mobile devices must be avoided and is allowed only in extenuating circumstances, as defined in the Appropriate Use Policy.

Minimum information protection safeguards for the use of mobile devices must include:

- Encryption of stored data to prevent information loss resulting from the theft of the mobile or remote device;
- Encryption of data transmitted via public network;
- Access control permissions on a mobile device to prevent unauthorized access to information by system users, particularly for multi-user mobile systems;
- Regularly maintained data backups of information stored on mobile devices using government backup facilities to protect against information loss;
- Physical security of the device at all times to protect against asset and information loss; and,
- User authentication to the mobile device and user authentication for remote access from the device in accordance with authentication policies.

Recommended Tests:

Note: ISP 2.2.1 is reported on as part of the annual information security review as CO.2.16.

- Demonstrate that Security Threat and Risk Assessments have been completed on mobile devices.
- Demonstrate that only approved mobile devices are in use.
- Demonstrate that all mobile devices are registered and regularly inventoried.
- Demonstrate that processes are in place to update software and apply patches.
- Demonstrate restricted access and that appropriate access controls are applied.
- Demonstrate that protection mechanisms such as cryptographic controls, malware protection and remote disabling/erasures are applied when available or required.

2.2.2 Teleworking must employ security controls to ensure that information resources are not compromised.
a) Teleworking security controls
b) Teleworking agreement
c) Ad hoc teleworking policy

Purpose: ***To protect information accessed through teleworking arrangements from loss or unauthorized access.***

2.2.2 a) Teleworking security controls based on risk assessment

Information Owners and Information Custodians must ensure that government information and information technology assets are adequately protected regardless of the type of access or physical location of employees. Teleworking security controls must consider:

- The sensitivity and classification of information assets that may be accessed or stored at the teleworking location (e.g., paper files, mobile devices such as laptops, smartphones, USB drives);
- The physical security of information, information technology assets and the teleworking location;
- Unauthorized information access by people at the teleworking location, either inadvertent or deliberate;
- Enrollment in Mobile Device Management Service;
- Remote access threats if remote access is utilized;
- Restriction of permitted information types and classifications at the teleworking location;
- Provision of government-managed equipment, if appropriate, due to information sensitivity or volume;
- Use of secure cabinets, shredders and other physical security equipment;
- Security awareness training for protection of information and information assets, including clear desk policy, information handling rules, physical security issues and remote access training; and,
- Monitoring and review of teleworking equipment for security events and incident response.

Sensitive and confidential information must be stored only on protected government systems, as defined in the Appropriate Use Policy.

2.2.2 b) Teleworking agreement

Teleworking arrangements must be formally authorized and documented.

A documented teleworking agreement between the employer and employee must exist that specifies the following employee responsibilities, terms and conditions:

- The expectation that the employee will actively protect information and information technology assets;
- Reference to the BC Public Service Agency Human Resource Policies, Oath of Employment, Standards of Conduct, Appropriate Use Policy, Information and Communications Technology (ICT) Agreement, or contract terms as appropriate;
- Restrictions on information asset types or classifications permitted at the teleworking location;
- The requirement to protect information from inadvertent or deliberate disclosure to people at the teleworking location by use of secure cabinets, passwords or shredders;
- The authorized teleworking location and contact information;
- Information availability requirements;
- What equipment and software is supplied by the employee and by the employer;
- Completion of a Home Technology Assessment;
- The terms of use for remote access, if applicable;
- The requirement to meet or exceed specified wireless networking security controls, if wireless networking will be used at the teleworking location;
- The requirement to report security events or unusual activity;
- Arrangements for technical support; and,
- The start date, end date, expected work hours and provision for termination of the teleworking arrangement.

2.2.2 c) Ad hoc teleworking policy

Ministries must develop and communicate policies and processes specific to their areas that govern ad hoc teleworking, in particular the practice of removing material from the workplace. Controls required for an ad hoc teleworking policy are:

- Restriction of the information asset types and classifications that may be accessed or utilized while teleworking;
- Use of secure cabinets, shredders and other physical security equipment; and,
- Minimum technical security controls required for non-government computing equipment, in particular current anti-virus, personal firewall and current software patches.

Guidelines:

Teleworking employees should use the following security measures when accessing government information services:

- Desktop Terminal Service (DTS) – preferred access method for non-government devices;
- DTS or Virtual Private Network (VPN) for government devices; and
- Application specific methods such as Secure Sockets Layer (SSL) enabled websites (e.g., Outlook Web Access).

Use of VPN access on non-government devices should be avoided, unless it is used with Remote Desktop Protocol (RDP) connection.

Recommended Tests:

Note: ISP 2.2.2 is reported on as part of the annual information security review as CO.2.18.

- Demonstrate teleworking policies and teleworking agreements are documented.
- Demonstrate Home Technology Assessments are completed.

3 Human Resource Security

This chapter identifies the information security requirements for employees that have an employment relationship with government organizations. To reduce information security risks, the terms and conditions of employment must establish expectations for the protection of government assets, information and services.

This chapter references the terms and conditions set by the BC Public Service Agency for employees and identifies the conditions for external personnel such as contractors.

Supervisors and employees have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish Supervisor responsibilities, education, training and formal processes to handle problematic security situations. This chapter also establishes rules to ensure a secure transition when employment is ended or changed.

3.1 Prior to employment

3.1.1	**Employee security screening must be performed prior to entering a working relationship with the Province.** **a) Screening for employees** **b) Screening for contractors**

Purpose: ***To verify employment qualification claims made by prospective employees.***

3.1.1 a) Screening for employees

The process for employee screening is detailed in BC Public Service Agency Human Resource Policies.

3.1.1 b) Screening for contractors

The process for contractor screening is detailed in Core Policy and Procedures Manual, Chapter 6 – Procurement.

Guidelines:

The process for contractor screening can be used to screen other individuals such as volunteers.

Applicants should be screened to assess their education, skills, knowledge, experience and past work performance. The screening should also confirm the applicant's identity. The extent of the screening process should be commensurate with the sensitivity of the information and nature of work to be performed.

Ministries may exempt applicants from the screening process where:

- Employees have been previously screened for similar types of government work within the last 2 years; or,
- The sensitivity of the information and nature of work to be performed does not warrant a complete screening process.

Ministries should maintain a list of contractors and other individuals who have been screened and the dates.

Recommended Tests:

Note: ISP 3.1.1 is reported on as part of the annual information security review as CO.3.2.

- Demonstrate that the provisions in the BC Public Service Agency Human Resources Policies, Security Screening have been followed.
- Demonstrate candidates for employment have confirmation of academic and professional qualifications.

3.1.2	**The terms and conditions of employment must document the responsibility of employees for information and information systems security.** **a) Terms and conditions of employment** **b) Communication of terms and conditions of employment** **c) Violation of terms and conditions of employment**

Purpose: ***To establish the terms and conditions of employment for information and information systems security.***

3.1.2 a) Terms and conditions of employment

The terms and conditions of employment are defined in the BC Public Service Agency, Human Resource Policies, the Oath of Employment and the Standards of Conduct.

The terms and conditions of employment defined in contracts must include:

- Legal responsibilities and rights (e.g., laws relating to intellectual property rights, freedom of information, and privacy);
- Confidentiality requirements that include responsibilities for the handling and storage of information assets; and,
- Consequences of failing to adhere to the terms and conditions.

3.1.2 b) Communication of terms and conditions of employment

Supervisors must ensure terms and conditions of employment are agreed to by employees prior to employment or provision of services, including signing the Oath of Employment and receiving a copy of the Standards of Conduct.

3.1.2 c) Violation of terms and conditions of employment

Employees in violation of the terms and conditions of employment are subject to disciplinary action including dismissal, cancellation of contract or other legal remedies.

Recommended Tests:

Note: ISP 3.1.2 is reported on as part of the annual information security review as CO.3.6.

- Demonstrate that employment agreements reflect information security responsibilities.
- Demonstrate contractors are made aware of information security responsibilities.
- Demonstrate that the responsibilities for information and information systems security are included in the employment terms and conditions.

3.2 During employment

3.2.1	**Supervisors must ensure employees comply with information security policies and procedures.** **a) Supervisor responsibilities** **b) Review of security roles and responsibilities**

Purpose: ***To establish Supervisor responsibilities for ongoing support and implementation of information security.***

3.2.1 a) Supervisor responsibilities

Supervisors must support the implementation of information security policies and practices by:

- Ensuring employees are informed of information security roles and responsibilities prior to being granted access to information or information systems;
- Supporting and encouraging employees to adhere to information security policies; and,
- Requiring that employees conform to the terms and conditions of employment, including information security policies.

3.2.1 b) Review of security roles and responsibilities

Information security roles and responsibilities must be reviewed when staffing or restructuring public service or contract positions, or when implementing new, or significant changes to, information systems.

Guidelines:

Supervisors should annually review and validate information security roles and responsibilities in job descriptions, standing offers, contracts and information usage agreements.

Recommended Tests:

Note: ISP 3.2.1 is reported on as part of the annual information security review as CO.3.10.

- Demonstrate that employees are provided guidelines stating information security expectations.
- Demonstrate that awareness programs are provided on information security roles and responsibilities.
- Demonstrate that any contracts not using the General Services Agreement express the requirement to abide by government policy.
- Demonstrate Supervisors ensure that employees participate in mandatory and ongoing information security awareness and training opportunities (e.g., Public Service Agency courses, Security Days).

3.2.2	**Employees must receive appropriate information security training and be informed of changes to information security policy and practices.** **a) Orientation for new employees** **b) Ongoing information security awareness, education and training**

Purpose: ***To increase employee awareness and understanding of security threats, risks and concerns and information security policies and procedures.***

3.2.2 a) Orientation for new employees
Supervisors must include an information security awareness component in orientation processes that employees must complete prior to accessing information or information systems.

3.2.2 b) Ongoing information security awareness, education and training
Supervisors must provide ongoing information security awareness, education and training, addressing topics including:

- Protection of information;
- Information privacy requirements;
- Records management;
- Known information security threats;
- Legal responsibilities;
- Information security policies and directives;
- Reporting information security events;
- Appropriate use of government resources;
- Technology training;
- Information on disciplinary processes; and,
- How to obtain security advice.

Guidelines:
Resources on information security awareness, education and training are available from:

- Ministry Information Security Officers;
- Ministry Privacy Officers;
- Corporate Information and Records Management Office;
- The Chief Information Security Officer, OCIO; and,
- Awareness section of the Information Security Branch, OCIO.

Recommended Tests:
Note: ISP 3.2.2 is reported on as part of the annual information security review as CO.3.12.

- Demonstrate an information security awareness program is in place, is active and has wide participation.
- Demonstrate that employees are delivered regular awareness education in their program areas of responsibility.
- Demonstrate Executive level support for information security awareness training and education.

3.2.3 Security breaches or policy violations caused by employees must be reviewed by Supervisors.
a) Reviewing security breaches and policy violations

Purpose: ***To ensure a process is in place to review the activities of employees who commit an information security breach or policy violation.***

3.2.3 a) Reviewing security breaches and policy violations
Upon receipt of information identifying employees responsible for a potential or actual security breach or policy violation, Supervisors are responsible for:

- Ensuring the Ministry Chief Information Officer has been informed of the outcome of the security incident and investigation;

- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining, in consultation with the BC Public Service Agency, if disciplinary action is warranted for employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

Recommended Tests:

Note: ISP 3.2.3 is reported on as part of the annual information security review as CO.3.14.

- Demonstrate that Supervisors are aware of the procedures required to report security incidents to the Office of the Government Chief Information Officer.
- Demonstrate that appropriate steps are taken to preserve forensic evidence for investigators.

3.3. Termination or change of employment

3.3.1 Responsibilities for employment termination must be documented.
a) Termination of employment responsibilities

Purpose: ***To ensure information security responsibilities upon termination of employment are defined and assigned.***

3.3.1 a) Termination of employment responsibilities

Supervisors must advise employees of ongoing confidentiality responsibilities that continue to apply after termination of employment, as outlined in the Standards of Conduct.

Recommended Tests:

Note: ISP 3.3.1 is reported on as part of the annual information security review as CO.3.18.

- Demonstrate that employees have been made aware of confidentiality requirements following termination.

4 Asset Management

Information and information systems services constitute valuable government resources. The asset management chapter establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

To account for the assets that require protection, this chapter specifies the requirement to designate who owns assets. Designated owners become responsible for protecting information and technology assets and to maintain the way assets are protected.

This chapter sets the foundation for a system that classifies information to identify different security levels, to specify how much protection is expected and how information should be handled at each level. Not all information requires the same level of protection because only some information is sensitive or confidential.

4.1 Responsibility for assets

4.1.1	**An inventory of all important assets associated with information systems must be documented and maintained.** **a) Identification of assets** **b) Documenting and maintaining asset inventories** **c) Loss, theft or misappropriation of assets**

Purpose: ***To identify organizational information assets and define appropriate protection responsibilities.***

4.1.1 a) Identification of assets

Information Owners must identify assets under their control including:

- Software;
- Hardware including mobile devices and tablets;
- Services including computer and communications services and general utilities;
- Information assets required to be inventoried in the personal information directory (required under the Freedom of Information and Protection of Privacy Act); and,
- All other information assets including: database and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, and archived information.

4.1.1 b) Documenting and maintaining asset inventories

Information Owners and Information Custodians must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of an enterprise risk management strategy.

Information Owners and Information Custodians must document, maintain and verify the personal information directory including the personal information bank and privacy impact assessment sections.

The following information should be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss, disposal or destruction:

- Type of asset;
- Ownership;
- Format;
- Location;
- Back-up information and location;
- Licence information;
- Sensitivity and safeguards requirements;
- Criticality for service delivery and maintaining business functions; and,
- Consequences of loss.

Information Owners and Information Custodians are accountable for asset identification and inventory maintenance.

4.1.1 c) Loss, theft or misappropriation of assets
The loss, theft or misappropriation of assets must be reported immediately using the General Incident or Loss Report. Where the loss, theft or misappropriation involves information, the Information Incident Management Process must be followed.

Recommended Tests:
Note: ISP 4.1.1 is reported on as part of the annual information security review as CO.4.4.

- Demonstrate that assets are identified and tracked throughout the asset's life-cycle, i.e., creation, processing, storage, transmission, deletion, and disposal.
- Demonstrate the inventory of information assets is regularly inspected for correctness.
- Demonstrate information assets are properly classified and the criticality of the asset is identified.
- Demonstrate Executive support in asset management.
- Demonstrate information incidents and loss of assets are reported immediately.

4.1.2	**Information Owners and Information Custodians must be designated for all assets associated with information systems.** **a) Responsibilities for asset ownership** **b) Designating Information Custodians**

Purpose: ***To designate custodians for assets, with approved management responsibility, for the protection of organizational assets associated with information and technology systems or services.***

4.1.2 a) Responsibilities for asset ownership
All information assets must have a designated owner.

An Information Owner is responsible for controlling the production, development, maintenance, use and security of information and technology assets within their jurisdiction. Information Owners are responsible for:

- Ensuring the appropriate classification and safeguarding of information and technology systems or services;
- Defining and regularly reviewing access restrictions, classifications and safeguards in accordance with applicable policies; and,

- Designating Information Custodians and ensuring that they have the correct tools for protecting designated assets.

4.1.2 b) Designating Information Custodians
Information Owners may delegate responsibility for custody of information and technology systems or services to Information Custodians.

Information Custodians will be responsible for:
- Overseeing the functioning of information and technology assets;
- Delivery of services in accordance with defined service requirements; and,
- Regular reporting on designated information and technology assets.

Guidelines:
Ownership and custodianship responsibilities should be defined and monitored within the employee's Performance Management tool "MyPerformance Profile".

Recommended Tests:
Note: ISP 4.1.2 is reported on as part of the annual information security review as CO.4.6.
- Demonstrate that ownership is reflected in the information assets inventory.
- Demonstrate owners have considered access restrictions, classification, safeguards and handling for information assets.
- Demonstrate regular reporting status of information assets to the owner.
- Demonstrate ownership in security reviews (e.g., Security Threat and Risk Assessments, Privacy Impact Assessments).

4.1.3 Rules for the acceptable use of information systems must be identified, documented and implemented.
a) Acceptable use of government resources

Purpose: ***To prevent misuse or compromise of government information systems.***

4.1.3 a) Acceptable use of government resources
All users of government information systems must take responsibility for, and accept the duty to actively protect, government information and technology assets.

The requirements and terms of use of government information systems, including personal use, are described in CPPM Section 12.3.1 - Appropriate Use of Government Information and Information Technology Resources (Appropriate Use Policy).

Recommended Tests:
Note: ISP 4.1.3 is reported on as part of the annual information security review as CO.4.8.
- Demonstrate employees accessing information assets are aware of the Appropriate Use Policy.
- Demonstrate supervisors authorize the downloading of applications and software.
- Demonstrate employees are familiar with the responsibilities for information asset loss reporting.

4.1.4	**Employees must return government assets upon termination or change of employment.** **a) Return of assets**

Purpose: ***To ensure employees return physical and information assets at termination or change of employment.***

4.1.4 a) Return of assets

Supervisors must document the return of government assets in the possession of employees upon termination of their employment using standard processes. These processes must ensure the:

- Return of:
  - documents, files, data, books and manuals in physical or other media formats including other information assets developed or prepared by an employee or contractor in the course of their duties,
  - computer hardware, software and equipment (e.g., mobile devices, portable media), and,
  - access devices, cards, vouchers and keys (e.g., credit cards, taxi cards, travel vouchers);
- Returned items are verified against established asset inventories;
- Recovery or compensation for assets not returned, based on established criteria regarding depreciation and replacement value for classes of items; and,
- Identification of unreturned access devices, cards and keys that could permit unauthorized access or alteration, disposal or destruction of assets, so that information and security systems can be protected.

Recommended Tests:

Note: ISP 4.1.4 is reported on as part of the annual information security review as CO.4.10.

- Demonstrate the information asset inventory is reviewed for all assets on loan at termination.
- Demonstrate a formal procedure to recover information assets at termination, including document files, electronic storage devices, computers, mobile devices, access cards and/or keys.

4.2 Information classification

4.2.1	**The government information security classification system must take into account the value, sensitivity and intended use of the information.** **a) Information and information system security classification** **b) Mandatory features of information security classification** **c) Mandatory features of information system security classification**

Purpose: ***To define the information security classification system characteristics for information and information systems.***

4.2.1 a) Information and information system security classification

Information Owners and Information Custodians must use the Information Security Classification system to categorize information and information systems.

The Office of the Government Chief Information Officer is responsible for definition, application and enforcement of the Information Security Classification system.

Risk Management Branch and Government Security Office is responsible for definition of Security Categories.

4.2.1 b) Mandatory features of information security classification

The Information Security Classification system must:

- Apply to information types rather than discrete data elements;
- Determine the relative value of information including factors such as:
  - Statutory or regulatory requirements,
  - Impact to health, life or personal safety,
  - Effects of data aggregation,
  - Impact to the Ministry service plan from loss of information confidentiality, integrity and availability, and,
  - Changes to information sensitivity over time;
- Maintain compatibility with the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS).

The Information Security Classification system must include processes for:

- Defining information types for categorization;
- Making decisions on categorization of information; and,
- Periodic reassessment of the information security categorization processes.

4.2.1 c) Mandatory features of information system security classification

The Information Security Classification system must include processes for:

- Categorization of information systems based on the security classification of information stored, handled or processed by the information system; and,
- Inclusion of information and system security classification documentation in the System Security Plan.

Guidelines:

The Information Security Classification system is a cornerstone of security and risk assessment activities. The security categories communicate the value and classification of information in a way that allows for decisions to be made about risk management and information handling.

Information Security Classifications assist in:

- Consistent, comparable Statement of Sensitivity descriptions of the Security Threat and Risk Assessment describing the confidentiality, integrity and availability requirements of the assessed system.
- The selection of system security controls - service providers can bundle system security controls into packages or service offerings based on the consistently defined protection requirements of the information.
- The selection of, and consistent application of, information handling and labeling rules.
- Information sharing agreements by indicating the relative value of information being exchanged in a consistent and comparable manner across government.

Recommended Tests:

Note: ISP 4.2.1 is reported on as part of the annual information security review as CO.4.14.

- Demonstrate that information applications and information technology have Security Threat and Risk Assessments completed that consider information classification.
- Demonstrate that personal information has a Privacy Impact Assessment conducted.
- Demonstrate that classified information is processed, handled, stored and transmitted according to information classification sensitivity.
- Demonstrate that an injury or harm test is completed on information to determine proper classification.
- Demonstrate that information security classification is applied across the Ministry.

4.2.2 Information must be identified, labelled when appropriate and handled in accordance with the assigned information security classification.
a) Information labelling procedures
b) Information handling procedures

Purpose: ***To protect information in accordance with its security classification.***

4.2.2 a) Information labelling procedures

Information Owners and Information Custodians must document procedures to label information with its information security classification as required by the government Information Security Classification system. Information labelling communicates the security classification and protection requirements to employees.

Information types that must be considered for labelling include: printed or electronic records, reports, files, on-screen displays or messages. Information Owners must select and document the appropriate label type for each information type.

Automatic information labelling must be used where possible (e.g., by use of document templates, standard report footers, printer watermarks, on-screen displays, or system-applied text).

Where direct information labelling is not possible, alternate methods must be used to communicate the information security classification, such as marking storage media, description in information sharing agreements or system interface specifications, or use of metadata.

4.2.2 b) Information handling procedures

Information Owners and Information Custodians must document information handling procedures for secure processing, storage, transmission, declassification and disposal of information assets.

Information protection procedures must take into account the information security classification, labelling and handling processes and the access control policies.

Procedures must be defined for interpreting information security classification labels from, and handling information exchanged with, other jurisdictions.

Guidelines:

During systems development, specify the information security labelling requirements when defining business requirements for reports, screens and data storage.

Recommended Tests:

Note: ISP 4.2.2 is reported on as part of the annual information security review as CO.4.16.

- Demonstrate information in all formats is labeled in accordance with the sensitivity.
- Demonstrate all media formats can be marked with appropriate sensitivity labels.
- Demonstrate labeling is automated with the use of templated documents when appropriate.

4.2.3	**Information assets must be handled and stored so as to prevent unauthorized information disclosure or misuse, in accordance with the information security classification system.** **a) Asset handling procedures** **b) Media handling procedures**

Purpose: ***To ensure that documented procedures are used for handling information assets and storage of media in accordance with the security classification of information stored on the media.***

4.2.3 a) Asset handling procedures

Information Owners and Information Custodians must follow the procedures for information security classification when handling information assets.

The following items must be considered when dealing with information assets:

- Access restrictions supporting the protection requirements for each level of classification;
- Protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
- Storage of IT assets in accordance with manufacturers' specifications; and,
- Clear marking of all copies of media for the attention of the authorized recipient.

Information sharing agreements must include:

- Procedures to identify the classification of that information;
- Interpretation of the classification labels from other organizations; and,
- Level of protection required.

4.2.3 b) Media handling procedures

Information Owners and Information Custodians must document media handling procedures that are compliant with the information security classification and handling requirements for information stored on the media. If information of various security classifications is stored on media, the media must be handled according to the highest classification of the information stored.

Media handling documentation must include procedures for:

- Marking of media to its highest information classification level label, in order to indicate the sensitivity of information contained on the media;
- Access control restrictions and authorization;
- Correct use of technology (e.g., encryption) to enforce access control;
- Copying and distribution of media, including minimization of multiple copies, marking of originals and distribution of copies;
- Operating the media storage environment and managing media lifespan according to manufacturer specifications;
- Regular status accounting of media;

- Maintenance of media transfer and storage records;
- Media destruction and disposal; and,
- Employee training.

Only approved media devices appropriate for the classification of the information being stored must be used.

Recommended Tests:
Note: ISP 4.2.3 is reported on as part of the annual information security review as CO.4.18.

- Demonstrate access restrictions support the classification of assets.
- Demonstrate procedures are in place for storage of classified assets commensurate with the sensitivity label.
- Demonstrate transmission considerations are based on classification (e.g., highly sensitive material is not placed in the mail but instead a bonded courier is utilized).

4.3 Removable media

4.3.1	**All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media.** **a) Management of government records** **b) Use of portable storage devices** **c) Human factors** **d) Risk assessment factors and controls** **e) Mandatory controls**

Purpose: ***To ensure that risks to information introduced by portable storage devices are managed.***

4.3.1 a) Management of government records
Corporate Information and Records Management Office is responsible for the management and disposal of government records according to records schedules approved under the Information Management Act.

4.3.1 b) Use of mobile or portable storage devices
The use of mobile or portable storage devices to store or transport information increases the risk of information compromise. These devices are typically small, and are easily lost, stolen or damaged, particularly when transported in public environments. Mobile or portable storage devices include, but are not limited to, USB drives, external hard drives, smartphones, tablets, laptops, and mp3 players.

Information Owners, Information Custodians and Supervisors must:

- Ensure that use of mobile or portable storage devices is managed and controlled to mitigate risks;
- Document processes for authorizing use of mobile or portable storage devices; and,
- Ensure employees using mobile or portable storage devices protect information and information technology assets in their custody or control.

Information Owners or Information Custodians must conduct a Security Threat and Risk Assessment on mobile devices or mobile computing services to determine the risk profile and suitability of the device or the service for government use prior to deployment within government.

Technical standards for each device type must be documented including product name, mandatory controls, permitted information classifications and strength of controls such as encryption key length. Device handling procedures should include instructions to minimize the amount of information stored on mobile or portable storage devices.

4.3.1 c) Human factors

Information Owners, Information Custodians and Supervisors must ensure employees using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with the required protection technologies and when they must be used; and,
- Familiar with the Information Incident Management Process and General Incident or Loss Reporting procedures.

4.3.1 d) Risk assessment factors

The Security Threat and Risk Assessment must consider the impact of disclosure or loss of information stored on portable media from threats such as:

- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media disposal or destruction;
- Improper long term storage environment;
- Exposure to malware; and,
- Incomplete erasure of data prior to device disposal.

Information classification and sensitivity levels must be considered in the risk assessment.

4.3.1 e) Mandatory controls

Minimum information protection safeguards for the use of portable storage devices must include:

- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Documented definition of information classifications or sensitivities permitted to exist on specific media types;
- Not storing the only version of a document on portable storage devices;
- Documented authorization processes for use of portable storage devices;
- Encryption of stored data;
- Contractual requirements for external parties that transport, handle or store portable storage devices; and,
- Adherence to manufacturer specifications for use of portable storage devices.

Documented portable storage devices handling procedures include:

- Off-site storage;
- Third party transportation;
- Information backup;
- Protection against malware;

- Logging of media custody and location to allow for accounting and audit;
- Media labelling to indicate owner, classification and special handling restrictions;
- Maintenance of information where the information storage requirement exceeds the expected media lifetime; and,
- Secure erasure and disposal.

Recommended Tests:
Note: ISP 4.3.1 is reported on as part of the annual information security review as CO.4.22.

- Demonstrate portable storage devices are stored commensurate with the classification of the information they contain.
- Demonstrate that cryptographic controls are applied for sensitive material storage.
- Demonstrate that procedures are in place to scan portable storage devices for malware.

4.3.2 Media must be disposed of securely and in a manner appropriate for the sensitivity of the data it contains.
a) Secure disposal and destruction of media

Purpose: ***To ensure that information cannot be retrieved from media that is no longer in use.***

4.3.2 a) Secure disposal and destruction of media
Any asset capable of storing electronic information is considered a type of media, including mobile and portable storage devices, hard disks, CDs, DVDs, and tapes. Information Owners and Information Custodians must ensure that media that is no longer required operationally (e.g., due to expiry, surplus, damage or wear), is disposed of securely. Prior to disposal, the Ministry Records Officer must be consulted.

Media disposal procedures must:

- Be documented and communicated to employees;
- Specify erasure and disposal measures whose strength is based on information sensitivity and type of media (e.g., erasure software);
- Include secure disposal or destruction of media if erasure is not sufficient, or not cost effective (e.g., destruction by shredding, incineration or chemical dissolution);
- Include secure storage measures for media collected for and awaiting erasure or disposal, to avoid undetected theft of small amounts of media from large volumes awaiting disposal; and,
- Include audit logs of media disposal.

Corporate Information and Records Management Office is responsible for ensuring secure disposal services are available to Information Owners and Information Custodians.

Guidelines:
A Corporate Supply Arrangement exists for provision of secure media disposal services. Secure disposal service companies should be used where practical to perform media disposal. Contact the Ministry Records Officer for further details.

Recommended Tests:
Note: ISP 4.3.2 is reported on as part of the annual information security review as CO.4.24.

- Demonstrate that Ministries have documented and validated erasure procedures to ensure a thorough erasure of removable media commensurate with the sensitivity classification.
- Demonstrate all removable media marked for disposal is logged, tracked and kept secure (locked cabinet, safe room).
- Demonstrate that assets are removed from inventory at time of disposal and proper records are maintained.
- Demonstrate that employees are aware of secure media handling and disposal procedures.

4.3.3 Media being physically transported must be appropriately protected.
a) Media transport procedures

Purpose: ***To protect information from unauthorized disclosure or loss during physical transport of media.***

4.3.3 a) Media transport procedures

The Office of the Government Chief Information Officer must document and implement security measures for the protection of media during transport that meet information classification and handling requirements. If information of various classifications is stored on media, the media must be protected according to the highest classification of the information stored.

Minimum media transport requirements are:

- Using couriers that are approved by government;
- Inspecting identification credentials of couriers upon pickup and delivery of packages;
- Obtain and retain receipts for media shipments;
- Using packaging that will protect the media from loss or damage; and,
- Packaging so that the classification of the media is not displayed.

Responsibility for specification of physical transport procedures are shared between Corporate Information and Records Management Office and the Risk Management Branch and Government Security Office.

Guidelines:

Where supported by a Security Threat and Risk Assessment, additional controls to protect media during transport include:

- Using notifications of transport activities, such as:
  - sender informing receiver of the impending shipment, and,
  - receiver confirming receipt of the shipment;
- Using two layers of packaging where the inner layer indicates the classification and handling requirements; and,
- Using a locked container.

Recommended Tests:

Note: ISP 4.3.3 is reported on as part of the annual information security review as CO.4.26.

- Demonstrate shipment logs are maintained and tracked to ensure delivery.
- Demonstrate that physical transport requirements are followed to prevent unauthorized disclosure or loss of media.

5 Access Control

This chapter identifies the controls that restrict access to government information and information assets. Access control protects organizations from security threats such as internal and external intrusions. The controls are guided by legislation that protects particular types of information (e.g., personal and other types of confidential information) and by business requirements.

Access control policies provide the blueprint for the management of employee access, authorizations and control requirements for computer networks, operating systems, applications and information. This chapter identifies security best practices and responsibilities for administrators and employees.

5.1 Business requirements of access control

5.1.1	**Access to information systems and services must be consistent with business needs and be based on security requirements.** **a) Access control policy** **b) Access control policy management** **c) Review of access control policy**

Purpose: ***To ensure that information and information systems are available for authorized use and protected from unauthorized use.***

5.1.1 a) Access control policy

Information Owners and Information Custodians are responsible for establishing, documenting and approving access control policies which must:

- Support and enable business requirements;
- Be based on requirements identified in Privacy Impact Assessments and Security Threat and Risk Assessments; and,
- Include classification of assets.

Access control policies must additionally:

- Consider both physical and logical access to assets;
- Apply the need-to-know and least privilege principles;
- Set default access privileges to deny-all prior to granting access;
- Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable;
- Have permissions assigned to roles rather than individual user identifiers; and,
- Access requirements should be determined at a functional, work unit level.

The access control policy must be communicated to employees as part of awareness training.

5.1.1 b) Access control policy management

Information Owners and Information Custodians are responsible for establishing processes to manage the access control policies, including:

- Ensuring the process is communicated to all employees;
- Documenting processes for employee registration and deregistration;

- Segregating roles and functions (i.e. access requests, access authorization, access administration);
- Defining rules for controlling access to privileged system functions;
- Identifying roles and/or functions which require multi-factor authentication; and,
- Identifying and justifying exceptional cases where there is a need for enhanced employee security screening for sensitive assets.

5.1.1 c) Review of access control policy

Information Owners and Information Custodians must conduct periodic reviews of the access control policies as part of an ongoing process for risk management, security, and privacy. Annual reviews are recommended. Reviews must be conducted:

- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes;
- When the threat environment changes or new vulnerabilities arise;
- Following significant government or Ministry re-organization as appropriate; and,
- For sensitive and business critical assets, reviews should be conducted more frequently than annually, based on the Security Threat and Risk Assessment.

Recommended Tests:

Note: ISP 5.1.1 is reported on as part of the annual information security review as CO.5.4.

- Demonstrate information sensitivity and classification is considered prior to granting access.
- Demonstrate segregation of duties for authorizing, and administering.
- Demonstrate review of access logs.

5.1.2	**Employees must only be provided access to the network services they have been specifically authorized to use.** **a) Access to network services** **b) Management controls and processes** **c) Means for accessing networks and network services**

Purpose: ***To support the information system access control policy by limiting network access to authorized users of specific information systems.***

5.1.2 a) Access to network services

Information Custodians must enable network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system.

5.1.2 b) Management controls and processes

Information Custodians must document processes for management of network access, including:

- Documentation and review of implemented network access controls;
- Identification of threats, risks and mitigation factors associated with network services;
- Testing of network access controls to verify correct implementation; and,

- Assisting Information Owners to verify the principle of least privilege is used to minimize access, as specified in the access control policy.

5.1.2 c) Means for accessing networks and network services
Information Custodians must define and implement:

- Permitted network access methods for each network zone (e.g., direct connection, Virtual Private Network, Wi-Fi, remote desktop connection, desktop terminal services); and,
- Minimum security controls required for connection to networks (e.g., patch levels, anti-virus software, firewalls, user and system authentication requirements).

Recommended Tests:
Note: ISP 5.1.2 is reported on as part of the annual information security review as CO.5.6.

- Demonstrate systems network access controls are implemented and tested to prevent unauthorized access.
- Demonstrate network security controls are in place and up-to-date to prevent unauthorized access.

5.1.3 Remote access to government information systems must be subject to authentication.
a) Remote access to government networks or services

Purpose: ***To identify and authenticate users and systems accessing the government network from remote locations.***

5.1.3 a) Remote access to government networks or services
Providers of remote network access services for individuals must:

- Perform a Security Threat and Risk Assessment for each remote access service to determine the authentication methods to be implemented. Factors to be considered include classification of network services, and information and information systems accessible from the remote access service;
- Require remote users to connect through government designated remote access services or security gateways (e.g., Virtual Private Network (VPN), Desktop Terminal Services (DTS), Outlook Web Access); and,
- Require user identification and authorization prior to permitting each remote network connection.

Providers of remote network access services for interconnection of networks must:

- Perform a Security Threat and Risk Assessment for each remote network interconnection to determine the user and system authentication methods to be implemented. Factors to be considered include:
  - classification of network services, information, and information systems accessible from the remote access service, and,
  - the strength of security controls implemented in the remote network;
- Obtain prior approval to interconnect networks from Information Owners of every information system accessible from the remotely connected networks; and,
- Require remote network interconnections to connect through government designated remote access services or security gateways (e.g., Virtual Private Network, Third Party Network Gateway).

Recommended Tests:

Note: ISP 5.1.3 is not reported on as part of the annual information security review.

- Demonstrate an approval been obtained from Information Owners prior to interconnecting networks.

5.1.4	**Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment.** **a) Authentication of connections**

Purpose: ***To increase assurance of system identification where required by system sensitivity or classification.***

5.1.4 a) Authentication of connections

Information Owners must use automatic equipment identification if the requirement is identified by a Security Threat and Risk Assessment. Factors to consider include:

- The sensitivity and classification of information that may be accessed or stored;
- The physical security of information, information technology assets and location;
- Unauthorized information access by people at the location, either inadvertent or deliberate; and,
- Remote access threats if remote access is utilized.

When Information Owners identify a requirement for connection to a network or information system from a specific location or equipment, the connection may be authenticated using automated equipment. Activities include:

- An identifier must be in, or attached to, the equipment;
- The identifier indicates that the equipment is permitted to connect to specified networks or information systems and must be maintained in the asset inventory;
- The equipment identifier must be inspected and sessions should be logged to verify that the identifier is being correctly used for access; and,
- Connections must be monitored to detect anomalies, such as unusual session times, overly long sessions, or increased frequency of use.

Good physical security is required to complement the use of equipment identifiers. Reliance should not be placed solely on automated equipment for authentication. The equipment should be secured from tampering by locating it inside a secure facility or ensuring it is under the direct supervision of an individual.

5.1.5	**Physical and logical access to diagnostic ports must be securely controlled.** **a) Protection of diagnostic ports**

Purpose: ***To prevent unauthorized use of maintenance or diagnostic facilities.***

5.1.5 a) Protection of diagnostic ports

To prevent bypassing of information system access controls, Information Custodians must implement access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed, and kept active for the minimum time required.

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized by agreements, contracts and conditions of use.

Use of diagnostic ports must be logged and monitored for suspicious activity.

Recommended Tests:
Note: ISP 5.1.5 is not reported on as part of the annual information security review.

- Demonstrate controls.

5.1.6	**The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system.** **a) Logical and physical network connection control** **b) Wireless networks**

Purpose: ***To control network connection in support of the access control policy and limit opportunity for unauthorized access.***

5.1.6 a) Logical and physical network connection control
Information Custodians must restrict the ability of users to physically and logically connect to networks according to the access control policy defined by Information Owners. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

Direct network connections to information systems must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to segregate it from direct network connections by employee workstations.

5.1.6 b) Wireless networks
Information Custodians must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a Security Threat and Risk Assessment.

Recommended Tests:
Note: ISP 5.1.6 is not reported on as part of the annual information security review.

- Demonstrate that network access is granted following the requirements for logical and physical separation.

5.1.7	**Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system.** **a) Network address control** **b) Control of routing information**

Purpose: ***To control network routing to prevent unauthorized access or bypassing of security control points.***

5.1.7 a) Network address control
Information Custodians must implement mechanisms to prevent unauthorized changes to network routing and traffic flow (e.g., through use of router access control lists).

Security gateways must be considered for network access control points, in accordance with information system security classification requirements. Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

5.1.7 b) Control of routing information
Information Custodians must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).

Recommended Tests:
Note: ISP 5.1.7 is not reported on as part of the annual information security review.

- Demonstrate network access control points.

5.2 Employee access management

5.2.1	**There must be a formal employee registration and de-registration process for granting access to all information systems.** **a) Registration** **b) De-registration**

Purpose: ***To ensure that all access actions are traceable to an identifiable individual or process.***

5.2.1 a) Registration
Information Owners and Information Custodians are responsible for managing access to the assets under their control and must implement registration processes which:

- Require approval for all access rights;
- Ensure access requests are approved by the Supervisor of the employee requesting access;
- Ensure the reasons for requesting access are consistent with job responsibilities;
- Maintain records of access right approvals;
- Ensure employees understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- Ensure access rights are consistent with the data uses documented in the approved Privacy Impact Assessment;

- Ensure accesses are traceable to an identifiable individual or process;
- Ensure each employee is assigned a single unique identifier for accessing information systems (See Exceptions section below);
- Ensure the responsibilities for authorizing access are segregated from the responsibilities for granting access;
- Restrict access by using predefined role permissions;
- Provide secure and separate transmission of the user identifier and password to the employee; and,
- In exceptional cases, where warranted by the classification of the asset and supported by a Security Threat and Risk Assessment, ensure enhanced employee security screening or background checks are completed prior to authorizing access.

5.2.1 b) De-registration

Information Owners and Information Custodians must formally assign responsibilities and implement processes to:

- Remove access privileges for employees no longer with the organization within 5 working days;
- Promptly review access rights whenever an employee changes duties and responsibilities;
- Promptly review access rights whenever the employee's branch or department is involved in significant reorganization;
- Review access privileges for employees on extended absence or temporary assignments within 10 working days of the change of status;
- Remove access privileges for employees terminated for cause concurrent with notification to the individual; and,
- Quarterly check for and remove inactive or redundant user identifiers.

Authority and Exceptions:

Individual employees may have multiple identifiers when:

- Required to meet limitations of technology (e.g., IDIR, MVS).
- Required to meet unique business requirements provided the rationale is documented and approved by the Information Owner or Information Custodian as appropriate.

Recommended Tests:

Note: ISP 5.2.1 is reported on as part of the annual information security review as CO.5.10.

- Demonstrate unique IDs are issued to employees and are documented.
- Demonstrate that exemption requests for shared IDs are current and are monitored.

5.2.2 A formal employee access provisioning process must be implemented to assign or revoke access rights for all user types to all systems and services.

Purpose: ***To ensure authorized user access and to prevent unauthorized user access to systems and services.***

5.2.2 a) Access provisioning process

Information Owners and Information Custodians must implement a formal employee access provisioning process. The provisioning process for assigning or revoking access rights granted to user IDs must include:

- Obtaining authorization from the owner of the information system or service for the use of the information system or service. Separate approval for access rights from management may also be appropriate;
- Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties;
- Ensuring that access rights are not activated (e.g., by service providers) before authorization procedures are completed;
- Maintaining a central record of access rights granted to a user ID to access information systems and services;
- Adapting access rights of employees who have changed roles or jobs and immediately removing or blocking access rights of employees who have left the organization; and,
- Periodically reviewing access rights with owners of the information systems or services.

Guidelines:
Employee access roles should be established based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews are more easily managed at the level of such roles than at the level of particular rights. Consideration should be given to including clauses in employees contracts and service contracts that specify sanctions if unauthorized access is attempted by employees.

Recommended Tests:
Note: ISP 5.2.2 is reported on as part of the annual information security review as CO.5.12.

- Demonstrate access is authorized by appropriate authorities prior to providing access and that authorization is specific to access rights.
- Demonstrate owners and/or their designate grant access based on business requirements.
- Demonstrate access is role based versus user based.

5.2.3 The allocation and use of system privileges must be restricted and controlled.
a) Managing, restricting and controlling the allocation and use of system privileges
b) Managing the issuance of privileged user credentials
c) Managing the issuance of multiple factors of authentication credentials

Purpose: To prevent unauthorized access to multi-user information systems.

5.2.3 a) Managing, restricting and controlling the allocation and use of system privileges
Information Owners and Information Custodians are responsible for authorizing system privileges and must:

- Identify and document the system privileges associated with each information system or service;
- Ensure the process for requesting and approving access to system privileges includes Supervisor approval(s) prior to granting of system privileges;
- Ensure processes are implemented to remove system privileges from employees concurrent with changes in job status (e.g., transfer, promotion, termination);
- Limit access to the fewest number of employees needed to operate or maintain the system or service;
- Ensure the access rights granted are limited to and consistent with employee job functions and responsibilities;

- Maintain a record of employees granted access to system privileges;
- Ensure use of system privileges is recorded in audit logs which are unalterable by the privileged user;
- Implement processes for ongoing compliance checking of the use of system privileges; and,
- Implement processes for regular review of authorizations in place to confirm that access is still needed and that the least number of users needed have access.

User identifiers with system privileges must only be used for performing privileged functions and not used to perform regular activities. User identifiers established to perform regular activities must not be used to perform privileged functions.

Guidelines:

- The design of information systems should include processes for performing regular maintenance activities which avoid the requirement of system privileges.
- Whenever possible system routines should be used to execute system privileges rather than granting system privileges to individual employees.
- System acquisition and development should encourage use of programs which minimize the need for employees to operate with system privileges.

Privileged users should:

- Not read the data of an information asset unless authorized;
- Be able to alter user permissions for an information asset; and,
- Be permitted to view, but not alter, user activity logs as part of security safeguards.

5.2.3 b) Managing the issuance and revocation of privileged user credentials

The issuance of privileged user credentials must have two levels of approval. Use of system privileges should require use of multi-factor authentication.

5.2.3 c) Managing the issuance of multiple factors of authentication credentials

The management of issuance of multiple factors of authentication credential is covered in the Cryptographic Standards for Information Protection.

Recommended Tests:

Note: ISP 5.2.3 is reported on as part of the annual information security review as CO.5.14.

- Demonstrate privileged users access is regularly reviewed to ensure access rights are in line with business requirements.
- Demonstrate that logs are regularly reviewed for privileged user activity.
- Demonstrate that when employees no longer require privileged access, it is removed.

5.2.4 The issuance and revocation of authentication credentials must be controlled through a formal management process.
a) Managing the issuance of authentication credentials

Purpose: To define the formal management processes for issuing passwords.

5.2.4 a) Managing the issuance and revocation of authentication credentials

Ministries must formally designate individuals who have the authority to issue and reset passwords. The following applies:

- Passwords must only be issued to employees whose identity is confirmed prior to issuance;
- Individuals with the authority to reset passwords must transmit new or reset passwords to the employee in a secure manner (e.g., using encryption, using a secondary channel);
- Whenever technically possible, temporary passwords must be unique to each individual and must not be easily guessable;
- Passwords must never be stored in an unprotected form;
- Default passwords provided by technology vendors must be changed to a password compliant with government standards during the installation of the technology (hardware or software); and,
- The revocation of authentication credentials must follow a formal process.

Recommended Tests:
Note: ISP 5.2.4 is reported on as part of the annual information security review as CO.5.16.

- Demonstrate that passwords are never stored or transmitted in clear text.
- Demonstrate employees are made aware to never divulge their password.
- Demonstrate that vendor provided equipment and software default passwords are changed upon implementation.

5.2.5 Information Owners must formally review employee access rights at regular intervals.
a) Circumstances and criteria for formal access right review
b) Procedure for formal access right review

Purpose: ***To ensure that access rights only exist for users with a defined "need to know".***

5.2.5 a) Circumstances and criteria for formal access right review
Information Owners and Information Custodians must implement formal processes for the regular review of access rights. Access rights must be reviewed:

- Annually;
- More frequently for high value information assets and privileged users;
- When an employee's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect an employee's need to access information assets;
- As part of a major re-organization, or the introduction of new technology or applications; and,
- When Information Owners change the access control policy.

5.2.5 b) Procedure for formal access right review
Review of access rights must include the following:

- Confirmation that access rights are based on the need-to-know and least privilege principles;
- Confirmation that all members of the group/role have a need-to-know;
- Reviews and verification of access control lists dated and signed by the reviewer and kept for audit purposes; and,
- Confirmation that changes to access rights are logged and auditable.

Access control logs and reports are government records and must be retained and disposed of in accordance with approved record management schedules.

Recommended Tests:

Note: ISP 5.2.5 is reported on as part of the annual information security review as CO.5.18.

- Demonstrate a regular review of all employee access rights are based on business requirements.
- Demonstrate reviews of access privileges for employees that have changed roles within the organization.
- Demonstrate changes to user access rights are logged.

5.2.6	**The access rights of employees to information systems must be removed upon termination of employment and reviewed upon change of employment.** **a) Change of employment status** **b) Action upon termination or change of employment** **c) Reduction of access rights**

Purpose: ***To ensure physical and logical access rights to information systems and information processing facilities are managed in relation to the security responsibilities of the job requirements.***

5.2.6 a) Change of employment status

Supervisors must review access to information systems and information processing facilities when employees change employment, including:

- When employees assume new roles and responsibilities;
- During restructuring of positional or organizational roles and responsibilities;
- When employees commence long-term leave; and,
- Updating directories, documentation and systems.

5.2.6 b) Action upon termination or change of employment

Supervisors must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment by:

- Removing or modifying physical and logical access;
- Recovering or revoking access devices, cards and keys; and,
- Updating directories, documentation and systems.

5.2.6 c) Reduction of access rights

Supervisors must ensure access to information systems and information processing facilities is reduced or removed before the employment terminates or changes, based upon the evaluation of risk factors such as:

- Whether the termination or change is initiated by the employee/contactor or by a Supervisor;
- The reason for termination;
- The current responsibilities of the employee/contractor; and,
- The value of the assets currently accessible.

Recommended Tests:

Note: ISP 5.2.6 is reported on as part of the annual information security review as CO.5.20.

- Demonstrate review of access to information systems and information processing facilities is conducted when employees change employment.
- Demonstrate access to information systems and information processing facilities is immediately removed upon termination of employment.

5.3 Employee responsibilities

5.3.1	**Employees must follow security best practices in the selection and use of passwords.** **a) Selection of passwords** **b) Password change** **c) Privileged accounts** **d) Protection and use of passwords**

Purpose: ***To maintain the integrity of the unique identifier (user id) by ensuring employees follow security best practices.***

5.3.1 a) Selection of passwords

When selecting passwords employees must:

- Select complex passwords, i.e., a mixture of characters as specified in the Standard;
- Keep authentication information confidential;
- Avoid recording authentication information; and,
- Avoid using the same password for multiple accounts.

The effectiveness of access control measures is strengthened when employees adopt security best practices for selecting passwords.

5.3.1 b) Password change

Passwords must be changed:

- During installation of hardware or software which is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If compromise has taken place or is suspected the incident must be reported in accordance with the Information Incident Management Process; and,
- In compliance with password change instructions issued by an automated process (e.g., password life-cycle replacement) or an appropriate authority.

5.3.1 c) Privileged accounts

Privileged accounts have wider and more powerful access rights to information assets. In addition to 5.3.1 a) and b), employees authorized to create or who hold privileged accounts must use passwords which are at least 15 characters where technically feasible.

5.3.1 d) Protection and use of passwords

Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing passwords;
- Permitting anyone to view the password as it is being entered;
- Writing down a password;
- Storing other personal identifiers, access codes, tokens or passwords in the same container;
- Keeping a file of passwords on any computer system, including mobile devices, unless that file is encrypted according to the Cryptographic Standards for Information Protection;
- Employing any automatic or scripted logon processes for personal identifiers; and,
- Using personal identifiers, access codes, or passwords associated with government accounts for non-government purposes.

Where a business need is defined to keep written records of passwords, a request for a policy exemption must be submitted to the Chief Information Security Officer.

Standards:
The Complex Password Standard for government systems requires that passwords must:

- Contain a minimum of 8 characters;
- Contain characters from three of the following categories:
  - English upper case characters (A to Z),
  - English lower case characters (a to z),
  - numerals (0 to 9), and,
  - non-alphanumeric keyboard symbols (e.g., ! $ # %); and,
- Not contain the username or any proper names of the employee.

For example, the complex password "T#ocitpi7"is derived from the phrase "The number of clowns in the parade is seven". Complexity can be further increased by substituting numbers for vowels.

For mobile devices connecting to the government messaging server, the following password rules apply:

- Passwords must contain a minimum of 6 characters;
- Controls should be in place to prevent the use of overly simple passwords; and,
- The use of a combination of numbers, symbols, upper and lower case characters is recommended to increase the password strength.

Guidelines:
Never divulge your password to anyone. Legitimate IT technical support employees such as systems administrators, helpdesk and security will not ask employees for their passwords.

Authority and Exceptions:
Exception is granted to RACF and VM Secure due to technical product limitations.

Recommended Tests:
Note: ISP 5.3.1 is reported on as part of the annual information security review as CO.5.24.

- Demonstrate password requirements are communicated to employees.
- Demonstrate an awareness program identifying employee password responsibilities.
- Demonstrate additional controls on privileged accounts.

5.4 System application access control

5.4.1	**Access to information systems functions and information must be restricted in accordance with the access control policy.** **a) Information access controls** **b) System configuration** **c) Publicly accessible information**

Purpose: ***To restrict access to application systems functions and information to authorized individuals or systems.***

5.4.1 a) Information access controls
Information Owners and Information Custodians are responsible for ensuring the implementation of the access control policy for their business applications. Every information system must have an access control policy that specifies access permissions for information and system functions. The access control policy must identify the information and system functions accessible by various classes of users.

The application and information section of the access control policy must specify:

- The information to be controlled;
- The system functions to be controlled; and,
- The roles authorized to access the resources and information and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

5.4.1 b) System configuration
Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.

System utilities or functions that can bypass user access controls must be specified in the access control policy. Access to these utilities and functions must be restricted.

5.4.1 c) Publicly accessible information
Information that is publicly accessible must be segregated from non-public information.

Recommended Tests:
Note: ISP 5.4.1 is reported on as part of the annual information security review as CO.5.28.

- Demonstrate access controls are implemented for application system functions.
- Demonstrate access control policies restrict access to powerful utilities and functions (e.g., role based access controls).
- Demonstrate access control policies segregate public information from non-public information.

5.4.2 Information systems managing data of a sensitive nature must have an isolated dedicated computing environment.
a) Segregation of sensitive information systems

Purpose: ***To ensure that sensitive information systems are segregated from non-sensitive information systems and are not compromised by sharing information technology resources with non-sensitive information systems.***

5.4.2 a) Segregation of sensitive information systems
Information Owners and Information Custodians must conduct a Security Threat and Risk Assessment to determine the information system classification level. The information system classification level determines which network security zone the information system must reside in.

Security zones must be established using physical or logical methods, which may include separate network segments, separate servers, firewalls, access control lists and proxy servers.

Recommended Tests:
Note: ISP 5.4.2 is reported on as part of the annual information security review as CO.5.28.

- Demonstrate the information system classification level has been determined.
- Demonstrate physical or logical security zones have been created.

5.4.3 Access to information systems must use a secure logon process.
a) Information displayed during logon
b) Unsuccessful logon attempts
c) Password transmission

Purpose: ***To ensure access to information systems is limited to authorized users and processes.***

5.4.3 a) Information displayed during logon

Information Owners must ensure that Information Custodians configure logon processes to minimize the opportunity for unauthorized access, which includes:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

5.4.3 b) Unsuccessful logon attempts

Information Owners must ensure that Information Custodians configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure, and if exceeded, the system should terminate the logon; and,
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

5.4.3 c) Password transmission

Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

Standards:

After three consecutive failed logon attempts for an account the logon process must:

- Lock the account and require Administrator intervention; or,
- Lock the account for 15 minutes and then allow a further three logon attempts.

Guidelines:

A general warning should be displayed that the information system is accessed only by authorized users.

The logon procedure should permit users to monitor the security of their account by displaying the following information on completion of a successful logon:

- Date and time of the previous successful logon; and,
- Details of any unsuccessful logon attempts since the last successful logon.

Recommended Tests:

Note: ISP 5.4.3 is reported on as part of the annual information security review as CO.5.30.

- Demonstrate critical business systems that process confidential/sensitive information within the Ministry (e.g., financial, personal information) are segregated appropriately by network zones, VLAN's.
- Demonstrate shared user identifiers are not used, as their use impedes investigation as to responsibility when multiple persons utilize the same credentials, and if for operational reasons there are shared identifiers an exemption must be obtained.
- Demonstrate successful and unsuccessful log on attempts are logged.
- Demonstrate that there is both a time maximum and minimum for logon attempts.

5.4.4	**All employees must be issued a unique identifier for their use only and an approved authentication technique must be used to substantiate the identity of the user.** **a) Allocation of unique identifier** **b) Authentication of identity** **c) Shared user identifiers**

Purpose: ***To ensure that access to information systems requires use of unique authenticated user identifiers.***

5.4.4 a) Allocation of unique identifier

Information Owners must ensure employees are issued unique user identifiers (user ids) for their use only, except as specified in 5.4.4 c). The documented and approved process for allocating and managing unique identifiers must include:

- A single point of contact to:
  - manage the assignment and issuance of user identifiers,
  - ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and,
  - record user status (e.g., employee, contractor);
- Identification of those individuals or positions authorized to request new user identifiers;
- Confirmation that the user has been informed of appropriate use policies;
- Automated linkages with the employees management system (i.e., CHIPS) to identify transfers, terminations and extended leave actions to initiate the suspension or cancellation of user identifiers;
- Linkages with contract management offices and/or contract managers to identify and maintain the status of identifiers issued to contractors; and,
- Conducting annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

5.4.4 b) Authentication of identity

Information Owners must ensure that user identifiers are authenticated by an approved authentication mechanism.

User identifiers authenticated by means other than a password must use a mechanism approved by the Office of the Government Chief Information Officer.

5.4.4 c) Shared user identifiers

In exceptional circumstances, where there is a clear business benefit identified by the Information Owner or Information Custodian, the use of a positional user identifier for a group of users or a specific job can be used, provided:

- Positional user identifiers are not used for privileged users; and,
- The Supervisor responsible for the position using the positional user identifier:
  - Maintains a record of the name of the individual, the user identifier, and the start and end date of use, and,
  - Deactivates the user identifier when not in use by requesting a password reset.

Guidelines:

Processes for issuing and managing information system user identifiers should be coordinated with those for issuing and managing other identification credentials (e.g., building passes, user identifiers for telecommunications services provided to an individual).

Recommended Tests:

Note: ISP 5.4.4 is not reported on as part of the annual information security review.

- Demonstrate annual reviews of all user identifiers conducted.
- Demonstrate notices of employee change received by user administrators within 5 working days.

5.4.5	**A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.** **a) Enforcing quality password rules**

Purpose: ***To support the operating system access control policy through use of password management systems to enforce the password standard.***

5.4.5 a) Enforcing quality password rules

Information Owners and Information Custodians must ensure password management systems:

- Enforce the use of individual user identifiers and passwords;
- Support selection and change of passwords using the Complex Password Standard (see ISP 5.3.1);
- Enforce change of temporary passwords at first logon and after password reset by an Administrator;
- Enforce regular user password change, including advance warning of impending expiry;
- Prevent re-use of passwords for a specified number of times;
- Prevent passwords from being viewed on-screen;
- Store password files separately from application system data;
- Ensure password management systems are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in protected (e.g., encrypted) form.

The password management system standard for government systems requires that users must be:

- Prevented from re-using the same password within 12 months; and,
- Provided with notification at least 10 days before their password will need to be changed.

Authority and Exceptions:

- Exception granted to RACF due to technical product limitations.
- Exemptions may be approved under specific criteria for non-expiring password usage. The Non-Expiring Password Acceptance Form is available from SSBC Client Resource Centre.

Recommended Tests:

Note: ISP 5.4.5 is reported on as part of the annual information security review as CO.5.32.

- Demonstrate systems not integrated with government's Active Directory (IDIR/BCeID authentication) need to determine if they are compliant with password integrity.
- Demonstrate passwords are not stored in clear text.
- Demonstrate systems found not compliant due to technical product limitations request an OCIO Policy / IM/IT Standards exemption record as evidence.
- Demonstrate user identifiers are authenticated by an approved authentication mechanism.

5.4.6 Use of system utility programs must be restricted and tightly controlled.
a) Restriction and control of system utility programs

Purpose: ***To restrict and tightly control the use of utility programs, which may be used to override system and application controls.***

5.4.6 a) Restriction and control of system utility programs

Information Owners and Information Custodians must limit use of system utility programs by:

- Defining and documenting authorization levels;
- Restricting the number of users with access to system utility programs;
- Annually reviewing the status of users with permissions to use system utility programs;
- Ensuring that the use of system utilities maintains segregation of duties;
- Requiring a secure logon process to be used to access system utilities;
- Ensuring that all system utility programs are identified and usage logged;
- Segregating system utilities from application software where possible; and,
- Removing or disabling unnecessary and obsolete system utilities and system software.

Guidelines:

Use of system utility programs should be limited to privileged users. Use of system privileges should require use of multiple factors of authentication.

Recommended Tests:

Note: ISP 5.4.6 is reported on as part of the annual information security review as CO.5.34.

- Demonstrate regular reviews of users authorized to access system utility programs.
- Demonstrate the segregation of duties for system utilities.
- Demonstrate logs are maintained and regularly reviewed for system utility programs.

5.4.7 Inactive sessions must be shut down after a defined period of inactivity.
a) Session time-out

Purpose: ***To ensure unattended information system sessions are automatically terminated.***

5.4.7 a) Session time-out
Information Owners and Information Custodians must define and implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity.

Government information systems must have session time-outs managed by operating system access, application or government infrastructure controls.

Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity commensurate with the:

- Risks related to the security zone;
- Classification of the information being handled; and,
- Risks related to the use of the equipment by multiple users.

The session must be terminated or require re-authentication after a period of no more than 15 minutes of inactivity.

Recommended Tests:
Note: ISP 5.4.7 is not reported on as part of the annual information security review.

- Demonstrate the maximum period of inactivity set to 15 minutes or less.

5.4.8	**Restrictions on connection times must be used to provide additional security for high value applications.** **a) Limiting access hours** **b) Limiting connection duration**

Purpose: ***To limit opportunities for inappropriate and unauthorized access to high value applications by restricting access hours and connection duration.***

5.4.8 a) Limiting access hours
Information Owners and Information Custodians must restrict access hours for high value applications. Restricting operating hours includes:

- Limiting access to pre-determined times (e.g., when Ministry support employees are available); and,
- Establishing restrictions for access from high risk public or external locations which are outside the control of the Ministry.

5.4.8 b) Limiting connection duration
Information Owners and Information Custodians must limit the duration of connection times for high value applications. Restricting connection duration includes:

- Limiting session length; and,
- Requiring re-authentication of the user when a session has been inactive for a pre-defined period of time.

Recommended Tests:
Note: ISP 5.4.8 is not reported on as part of the annual information security review.

5.4.9 Access control must be maintained for program source libraries.
a) Protection of program source libraries

Purpose: ***To protect information systems from unauthorized access or modification.***

5.4.9 a) Protection of program source libraries

Information Owners and Information Custodians must implement procedures to control access to program source code for information systems to ensure that:

- Program source code is isolated and stored separately from operational information systems;
- Privileged users access is defined and monitored;
- A change control process is implemented to manage updating of program source libraries and associated items;
- Program source code contained on any media must be protected; and,
- Accesses and changes to program source libraries are logged.

Recommended Tests:

Note: ISP 5.4.9 is reported on as part of the annual information security review as CO.5.36.

- Demonstrate that source code is not kept on production systems.
- Demonstrate that access to source code libraries is controlled and logged (e.g., reports from software development tools on code check-in and check-out).
- Demonstrate program source code is stored separately from operation information systems.
- Demonstrate program source code and program source libraries are managed according to established procedures.
- Demonstrate that access to all program source libraries is logged and regularly reviewed.

6 Cryptography

The use of cryptography for information controls needs to be based on the Security Threat and Risk Assessment and the level of harm caused by the loss of confidentiality and/or integrity. The cryptographic policies are under the direction of the Government Chief Information Officer.

6.1 Cryptographic controls

6.1.1	**The use of cryptographic controls must be based on the risk of unauthorized access and the classification of the information or information system to be protected.** **a) Cryptographic controls - Roles and responsibilities** **b) Acceptable use of cryptography**

Purpose: ***To manage the use of cryptography for protecting the confidentiality and integrity of electronic information.***

6.1.1 a) Cryptographic controls - Roles and responsibilities

The Government Chief Information Officer provides government direction and leadership in the use of cryptography and the provision of cryptographic services, such as those used for user registration services and key management services, by:

- Establishing policy and providing strategic direction on the use of cryptography across the organization;
- Instituting the approach to key management;
- Establishing roles and responsibilities;
- Setting standards for cryptographic algorithms and key length; and,
- Approving the use of cryptographic services.

The Chief Information Security Officer supports the use of cryptography in government by:

- Defining and maintaining the Cryptographic Standard for Information Protection; and,
- Providing technical advice on the use of cryptography.

Information Owners must document the use of cryptography in the System Security Plan for the information system.

6.1.1 b) Acceptable use of cryptography

The type and quality of cryptographic controls used in information systems must be based on a Security Threat and Risk Assessment, and include consideration of:

- Confidentiality requirements, in accordance with information classification, labelling and handling requirements;
- Integrity requirements (e.g., for financial payment instructions in excess of a specified dollar amount);
- Non-repudiation requirements (e.g., for proof of the occurrence or non-occurrence of an event);
- Authentication requirements (e.g., proof of identity);
- Other security measures (e.g., for proof of origin, receipt, or ownership);
- Legislation, regulations or policies requiring the use of cryptography;
- Restrictions on the export or use of cryptographic products; and,

- Risks relating to the long-term storage of electronic information (e.g., recovery of encrypted data, long-term key maintenance).

Information Owners and Information Custodians must register the use of approved cryptographic products and services with the Chief Information Security Officer.

Recommended Tests:

Note: ISP 6.1.1 is reported on as part of the annual information security review as CO.6.4.

- Demonstrate that the Information Owners and Information Custodians have considered the risk and types of encryption required for mobile devices.
- Demonstrate that the Information Owners and Information Custodians apply cryptographic controls approved by Chief Information Security Officer.

6.1.2 A key management system based on policy, procedures and approved methods must be used to support and protect the use of cryptographic controls throughout their life-cycle. a) Management of cryptographic keys

Purpose: ***To provide trustworthy key management processes for government cryptographic services.***

6.1.2 a) Management of cryptographic keys

The Government Chief Information Officer is responsible for approving key management standards and processes, including:

- Selection of cryptographic keys with sufficient lengths;
- Distribution, storage and periodic updating of cryptographic keys;
- Revocation of cryptographic keys (e.g., when a recipient changes job);
- Recovery of cryptographic keys that are lost, corrupted or have expired;
- Management of cryptographic keys that may have been compromised;
- Archival of cryptographic keys and the maintenance of cryptographic key history; and,
- Allocation of activation/de-activation dates.

Recommended Tests:

Note: ISP 6.1.2 is reported on as part of the annual information security review as CO.6.6.

- Demonstrate that cryptographic key management is approved by the Government Chief Information Officer and has a completed Security Threat and Risk Assessment for all sensitive information systems.

7 Physical and Environmental Security

This chapter identifies requirements for protection from environmental and man-made threats to employees and property. One of the principles used for protection is the use of a layered defence, with perimeters and security zones that place computers, people and information in secure areas.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the security of government information and information systems.

7.1 Secure areas

7.1.1	**Government information processing facilities must be protected by a physical security perimeter.** **a) Security perimeter** **b) Maintenance**

Purpose: ***To prevent unauthorized physical access to government information processing facilities.***

7.1.1 a) Security perimeter

Information Owners must ensure that the perimeters of an information processing facility are physically sound in design and consider landscaping, lighting, fencing, and closed circuit television on the access routes to the building; that the roof, walls and flooring are of solid construction; and that exterior access points, windows, and doors are equipped with appropriate security controls (e.g., locks, alarms, bars). All information processing facilities are a Restricted Access Security Zone.

Appropriate security controls must be applied to reduce the level of identified risks and include:

- A structure that prevents external visual and audio observations and complies with all applicable building codes for structural stability (external walls, internal walls, ceilings and doors). Walls surrounding the facility must be extended from true floor to true ceiling (slab to slab), to prevent unauthorized entry and minimize environmental contaminations such as that caused by fires and floods. Appropriate control mechanisms (e.g., locks, alarms and bars on windows and doors) must be applied to prevent unauthorized access;
- All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring employees to take immediate action;
- Information processing facilities must be equipped with doors that close automatically. These doors must set off an audible alarm when kept open beyond a certain period of time;
- All fire doors must be equipped with crash bars to allow a quick exit in the event of an emergency. When the doors are opened an audible alarm may also be set off;
- Alarm systems must be continuously monitored (i.e., 24 hours a day, 7 days a week); and,
- Government information processing facilities must be physically separated from those managed by third parties.

7.1.1 b) Maintenance

Information Custodians must review, and where appropriate test, physical security and environmental control requirements at least annually. Security requirements for facilities must be evaluated prior to significant:

- Alteration to exterior building layouts;
- Changes to perimeter security controls;

- Change in operations; and,
- As part of any related security incident investigation.

Guidelines:
The following guidelines support physical and environmental security by establishing perimeter security for information processing facilities:

- Information processing facilities should have a manned reception area to control access to the facility where feasible;
- Common service spaces such as eating areas, washrooms, cloakrooms, boardrooms and storage areas should be located so that they cannot be used to circumvent physical security;
- Visitor reception should be separate from entrance areas but provide an unobstructed view of the entrance; and,
- When physical security is outsourced, the contract must require that contracted employees are security screened and bonded.

Recommended Tests:
Note: ISP 7.1.1 is reported on as part of the annual information security review as CO.7.4.

- Demonstrate the perimeters of processing facilities are protected by intrusion devices.
- Demonstrate access to facilities is minimized and monitored (e.g., fire doors are alarmed).
- Demonstrate access to restricted zones is controlled (e.g., manned reception area, key-card access).
- Demonstrate regular review of information processing facility and records management storage rooms (e.g., computer data centre or telecommunications equipment room or records management office).
- Provide the annual security /environmental control review and inspect to ensure they have fulfilled this policy requirement.

7.1.2	**Secure areas must be protected by appropriate entry controls to ensure that only authorized employees are allowed access.** **a) Entry controls** **b) Maintenance**

Purpose: ***To prevent unauthorized physical access to government information.***

7.1.2 a) Entry controls
Information Owners and Information Custodians must establish the appropriate type and number of restricted zones to achieve the necessary conditions for employee safety, and for the protection of sensitive or valuable information and assets. Establishment of restricted zones must be supported by a Security Threat and Risk Assessment.

Access to any government information processing facility or areas where sensitive information is kept must be restricted. Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone. Entry controls must identify, authenticate and log all access attempts to a Restricted Access Operations Zone or a Restricted Access Security Zone as follows:

- Restricted Access Operation Zone access is limited to ministry employees and their escorted visitors (i.e., standard working areas, conference rooms, offices); and,

- Restricted Access Security Zone access is limited to authorized employees and their escorted visitors (i.e., communication closets, server rooms).

Every person authorized to enter a facility, including visitors, must be issued an identification badge that contains identifying information (such as name and photograph) and their level of building access. Badge colour or some other bold identifier may be used to represent the level of access.

- All badges must be checked prior to entry. A receptionist, security guard or electronic reader that logs the identity, time, date, and access privileges of each entry attempt must do such checking. Entry control may be achieved using keys, proximity card readers or other technologies;
- Employees must challenge anyone in a secure area who is not displaying an identification badge;
- Visitor or temporary access badges must be returned and accounted for at the end of each day;
- Entry logs must be reviewed on a quarterly basis;
- All entry logs must be secured and maintained according to the approved records retention schedule for the system or information asset; and,
- Access rights to secure areas must be reviewed and updated regularly.

When physical security is outsourced (i.e., the use of security guards) the contract must require that contracted employees are security screened and bonded.

7.1.2 b) Maintenance

Information Custodians are responsible for reviewing physical entry control requirements annually. All entry controls in place must be tested annually. Security requirements for facilities must be evaluated and a Security Threat and Risk Assessment completed prior to:

- Alteration to interior building layouts;
- Change to equipment/systems located in the facility;
- Change in operations; and,
- As part of any related security incident investigation.

Guidelines:

The following guidelines support physical and environmental security by establishing security within information processing facilities:

- Common service spaces such as eating areas, washrooms, cloakrooms, boardrooms and storage areas should be located so that they cannot be used to circumvent physical security;
- Visitor reception should be separate from entrance areas but provide an unobstructed view of the entrance; and,
- When physical security is outsourced, the contract must require that contracted employees are security screened and bonded.

The effective use of restricted access zones in an open office environment depends on the implementation of appropriate security procedures, which may include:

- Respecting the need-to-access principle and zone perimeters;
- Escorting visitors;
- Securing sensitive or valuable information and assets when leaving the work areas; and,
- Taking precautions when discussing sensitive information.

Recommended Tests:

Note: ISP 7.1.2 is reported on as part of the annual information security review as CO.7.6.

- Demonstrate that layered zones are employed to protect information and information processing facilities (e.g., reception zone, operation zone and security zone).
- Demonstrate that access to restricted operational and security zones employs controls that identify, authenticate and monitor all access attempts.
- Demonstrate that access controls and alarm systems have been implemented, and active monitoring is performed with log records retained.
- Demonstrate regular entry controls testing to determine if they meet the requirements.

7.1.3 Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility.
a) Physical security requirements

Purpose: ***To enhance physical and environmental security of information processing facilities by considering all security requirements during the design of the facility.***

7.1.3 a) Physical security requirements

Information Owners must design, document and approve security controls for information processing facilities based on a Security Threat and Risk Assessment. Considerations must include:

- Determining security perimeter and maintenance factors;
- Considering the operational use and information processing requirements of the facility;
- Establishing appropriate security zones;
- Design and construction complying with health and safety regulations and standards;
- Designed with environmental controls for the protection of information assets (e.g., fire suppression, HVAC, generators, alarms);
- Selecting unobtrusive sites and keep signage to the minimum required for meeting fire and other safety requirements;
- Limiting the identification of critical information processing facility locations, in publicly and internally available directories, to the minimum required; and,
- Selecting sites so that public access to highly sensitive or critical locations can be strictly controlled or avoided.

Recommended Tests:

Note: ISP 7.1.3 is reported on as part of the annual information security review as CO.7.8.

- Demonstrate layered physical security measures.
- Demonstrate Security Threat and Risk Assessment(s) completed to ensure the room(s) conforms to the Physical Security Technical Standards for Secure Zones.
- Demonstrate security controls methodology and documentation.
- Demonstrate public access to sensitive security zones is restricted.

7.1.4 Physical protection against natural disasters, malicious attacks or accidents must be designed and applied.
a) Design and site selection

Purpose: ***To enhance physical and environmental security by designing and applying physical security controls to mitigate damage from natural or man-made disaster.***

7.1.4 a) Design and site selection

Information Owners and Information Custodians, site planners and architects must incorporate physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural disasters, malicious attacks and accidents. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to meeting building code specifications and fire regulations, the following must be considered:

- Combustible or hazardous materials must be stored in purposely designed rooms and in appropriate containers;
- Installing intrusion detection and environmental alarm systems, fire suppression and firefighting systems must be included in the design phase; and,
- Fallback equipment (e.g., for Disaster Recovery Plan) and backup media must be sited at a safe distance to avoid damage from a disaster affecting the main site.

Recommended Tests:

Note: ISP 7.1.4 is reported on as part of the annual information security review as CO.7.10.

- Demonstrate regular inspections of the information processing facility by managers, fire and safety experts are performed to ensure the facility work areas and public areas are safe for occupants and equipment (e.g., intrusion and environmental alarm systems, fire suppression and firefighting systems are installed and functional).
- Demonstrate combustibles or hazardous materials are stored in approved containers separate from secure areas.
- Demonstrate appropriate alarms are situated for noxious gases, fire and flood and are monitored 24/7.
- Demonstrate system redundancy is sited at a safe distance in order to avoid damage affecting primary site.

7.1.5 Security controls and procedures must be used by employees working in secure areas.
a) Secure area requirements for employees
b) Other secure area requirements

Purpose: ***To prevent unauthorized physical access to government information by designing and applying additional security controls and procedures for employees working in secure areas.***

7.1.5 a) Secure area requirements for employees

Information Owners and Information Custodians must identify and document requirements that apply to employees authorized to work in secure areas. Information Owners must ensure that background checks including criminal records reviews are conducted for employees working in secure areas.

Information Owners and Information Custodians are responsible for informing employees working within a secure area that:

- Activities within a secure area are confidential and must not be discussed in a non-secure area - sensitive information must not be discussed with persons without a need-to-know;
- No type of photographic (including cameras in mobile devices), video, audio or other recording equipment is to be operated in a Restricted Access Security Zone unless authorized; and,
- Information security incidents must be reported immediately.

7.1.5 b) Other secure area requirements

Information Owners and Information Custodians must identify and document requirements for other individuals who may need access to a secure area. Information Owners and Information Custodians are responsible for ensuring that:

- Maintenance employees, cleaners and others who may require access on an ongoing basis to the secure area must be screened and their names placed on access lists;
- Visitors must obtain approval for visits, be screened, and their entry and departure times logged;
- Employees must escort visitors when they are within secure areas;
- Unoccupied secure areas must be physically locked and periodically checked; and,
- Physical intrusion alarms and detection devices must be installed to automatically alert monitoring employees of a breach.

Recommended Tests:

Note: ISP 7.1.5 is reported on as part of the annual information security review as CO.7.12.

- Demonstrate all employees who require access on an ongoing basis to secure areas are screened and their names placed on access lists; visitors obtain approval for visits, are screened, and their entry and departure times are logged.
- Demonstrate an escalation process to investigate any policy violations reported by the monitoring employees.
- Demonstrate controls for employees working within a secure area that include employees escort visitors when they are within the secure area; unoccupied secure areas are physically locked and periodically checked; physical intrusion alarms are installed to automatically alert monitoring employees of a breach.

7.1.6 Access to delivery and loading areas must be controlled, and where possible, separated from information processing facilities.
a) Controlling access to delivery and loading areas

Purpose: ***To prevent unauthorized physical access to government information by controlling access to delivery and loading areas and separating them from information processing facilities whenever possible.***

7.1.6 a) Controlling access to delivery and loading areas

Information Owners and Information Custodians, planners and architects must ensure that access to delivery and loading areas or access from Reception Zones is controlled when considering building design and specifications. The following factors must be considered:

- Delivery and loading areas must be designed so that supplies can be unloaded without delivery employees gaining access to restricted access zones;
- Protection of the delivery and loading areas must begin at the perimeter with continuous monitoring in place (e.g., gated fence, CCTV, separation from public access);
- Access to delivery and shipping areas must be restricted to authorized employees only;
- Setting and maintaining hours of operation for delivery and pick-up;
- A combination of internal and external locking doors or gates must be used to provide security;
- Incoming and outgoing shipments should be segregated when possible;

- Incoming material must be inspected for potential threats before being moved to or from the delivery and loading area. Inspections can be undertaken randomly if resources are not available to inspect every package;
- Hazardous materials must be appropriately packaged and identified as to safety precautions;
- Bills of lading must be compared to goods delivered;
- Loading docks and delivery areas must be regularly inspected and actively monitored;
- Records must be kept for internal and external deliveries and shipments;
- Reception areas must confirm the identification of all visitors for restricted zone access; and,
- All visitors must be accompanied while in restricted operational and security zones.

For facilities that include delivery and loading areas, and/or reception zones, a Security Threat and Risk Assessment and inspection must be conducted to determine that access can be adequately controlled.

Recommended Tests:
Note: ISP 7.1.6 is reported on as part of the annual information security review as CO.7.14.

- Demonstrate logs are maintained for all deliveries and shipments.
- Demonstrate reception areas, receiving and shipping areas are monitored for unauthorized access.

7.2 Equipment Security

7.2.1	**Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards.** **a) Equipment siting** **b) Equipment protection**

Purpose: ***To reduce risks to equipment from unauthorized access, environmental threats and hazards.***

7.2.1 a) Equipment siting
Information Owners, Information Custodians, planners, and architects must collaborate to ensure that the design and layout of information processing facilities provides protection for equipment from security threats as supported by a Security Threat and Risk Assessment. Safeguards must include:

- Locating servers and other centralized computing equipment within a Restricted Access Security Zone;
- Locating workstations, laptops and printers in a Restricted Access Operations Zone;
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas; and,
- Locating shared printers, scanners, copiers, and facsimile machines away from public or reception areas, or in passageways or other areas where employees who do not have a need-to-know can access printed material.

Information Owners and Information Custodians are responsible for ensuring that kiosks and public terminal safeguards are based on a Security Threat and Risk Assessment.

7.2.1 b) Equipment protection

Information Owners, Information Custodians, planners, and architects must collaborate to ensure that the design and layout of information processing facilities provides protection from physical and environmental hazards. Safeguards must include:

- Using equipment designed for suppression of electromagnetic emanations that may be used to capture information, when the need is supported by a Security Threat and Risk Assessment;
- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Providing lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Providing employees with approved eating and drinking areas separate from work areas containing equipment;
- Briefing employees who work with equipment about safety practices in the workplace and emergency equipment procedures to prevent an escalation in equipment damage;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems; and,
- Regularly inspecting the information processing facility(s) for integrity of ceilings, walls, windows, and other infrastructure for damage from water and other environmental factors that may pose a threat to safe equipment operation.

Recommended Tests:

Note: ISP 7.2.1 is reported on as part of the annual information security review as CO.7.18.

- Demonstrate the application of security zones.
- Demonstrate that equipment is properly sited and protected.
- Demonstrate temperature and heating are monitored to protect against adverse effects on equipment.
- Demonstrate that kiosk and public terminal safeguards are reviewed.
- Demonstrate that periodic inspections are conducted.

7.2.2	**Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.** **a) Planning and design** **b) Maintenance**

Purpose: ***To ensure continued availability by protecting equipment from disruptions caused by failures in supporting utilities.***

7.2.2 a) Planning and design

Information Owners and Information Custodians, planners, architects and engineers must collaborate in the planning and design of an information processing facility to ensure that supporting utilities (e.g., water, power, sewage, heating, ventilation) are adequate to support employees and systems that will be located in the facility. This includes estimating current and future utility capacity requirements for the facility. In addition to meeting the building code and other regulations, the following must be included in facility planning and specifications:

- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements;
- Emergency power off switches located near emergency exits in equipment rooms;
- Emergency lighting;
- Alarms to indicate inadequate water pressure for fire suppression;
- Alarms to indicate malfunctions in heating, ventilation, air conditioning, humidity control and sewage systems;
- Multiple connections to the power utility for critical systems and equipment;
- Multiple telecommunications connections to prevent loss of voice services; and,
- Adequate voice communications to meet regulatory requirements for emergencies.

7.2.2 b) Maintenance

Information Custodians must ensure that facilities are inspected regularly in accordance with building codes and other regulations. Evacuation and other emergency drills must be practiced regularly in collaboration with fire and emergency services. The facility requirements for utilities shall be re-evaluated:

- During the planning phase for replacing or changing existing technology hardware;
- When moving significant numbers of new employees into facilities;
- During the planning of renovations or major changes to an existing facility;
- Prior to leasing a facility; and,
- When there are major changes to the surrounding area that may affect utilities, evacuation routes or other safety aspects.

Recommended Tests:

Note: ISP 7.2.2 is reported on as part of the annual information security review as CO.7.20.

- Demonstrate redundancy in design for electric power, HVAC, water and communications.
- Demonstrate that Uninterrupted Power Supply (UPS) systems are tested regularly (e.g., monthly or quarterly), backup generators are tested regularly, and fuel supplies are maintained and replenished.
- Demonstrate facilities are inspected regularly in accordance with building codes and other regulations.
- Demonstrate evacuation and other emergency drills are practiced regularly in collaboration with fire and emergency services.

7.2.3	**Power and telecommunications cabling must be protected from interception and damage.** **a) Protection** **b) Inspection and monitoring**

Purpose: ***To ensure continued availability and integrity of information systems and information processing facilities by protecting power and telecommunications cabling from interception and damage.***

7.2.3 a) Protection

Information Owners and Information Custodians, planners and architects must include the protection of power and telecommunications cabling from interception and damage when designing or leasing facilities. The following methods to increase protection must be considered:

- Access to communication closets and server rooms must be highly restricted;

- Power and telecommunications cabling must be underground and/or in a secure conduit;
- Information cabling other than fibre optic must be protected with electromagnetic shielding when required;
- When supported by a Security Threat and Risk Assessment, consideration must be given to the use of fibre optics for telecommunications cabling;
- Cables must not be accessible in public areas;
- Power and telecommunications cabling must be segregated in accordance with building codes and other regulations; and,
- Inspection boxes, termination points, patch panels, control rooms and other facilities must be secured and located inside a Restricted Access Security Zone.

7.2.3 b) Inspection and monitoring

Information Custodians must ensure that:

- The integrity of power and telecommunications cables are monitored through regular inspections and reports;
- Power cabling and telecommunication schematics and documentation must be maintained in order to support inspections;
- Records of patches and other changes are maintained and inspected; and,
- Power and telecommunications cabling and wiring closets are inspected regularly and monitored for unauthorized access or inappropriate activity. The frequency of monitoring activities must be supported by a Security Threat and Risk Assessment.

Recommended Tests:

Note: ISP 7.2.3 is reported on as part of the annual information security review as CO.7.22.

- Demonstrate that the inspection of power and telecommunications cabling is performed annually.

7.2.4 Equipment must be correctly maintained to enable continued availability and integrity.
a) Routine maintenance
b) Maintenance of systems, hardware or media containing government information

Purpose: ***To ensure the continued confidentiality, integrity and availability of equipment through correct maintenance.***

7.2.4 a) Routine equipment maintenance

Equipment being repaired or maintained must be protected commensurate with the sensitivity of the information it contains and the value of the equipment. Information Owners and Information Custodians must determine if repair or maintenance can be conducted off-site. The need to protect sensitive information may justify equipment destruction and replacement rather than repair or maintenance.

Information Custodians are responsible for:

- Ensuring the scheduling of routine, preventive maintenance of equipment by qualified, authorized employees;
- Ensuring that maintenance is performed in accordance with the manufacturer's specifications, in compliance with warranty requirements, and using safe practices as specified in building codes, other regulations and insurance policies;

- Ensuring that, where possible, maintenance is scheduled to avoid interference with services or operations;
- Notifying affected employees prior to taking equipment off-line for scheduled maintenance;
- Ensuring that the value and sensitivity of the information contained on the device is considered prior to approval of off-site maintenance;
- Equipment sent for off-site maintenance must be inspected and logged out;
- Ensuring equipment returning from off-site repair or maintenance is inspected and logged in;
- Maintaining detailed records to identify trends, weaknesses and additional maintenance requirements which must include:
    - Place, date, time, type of scheduled maintenance and technical employees,
    - Suspected and actual faults identified,
    - Diagnostics performed and corrective action taken,
    - Unusual or unexpected events, such as early failures or breakdowns, and,
    - Any other event that requires maintenance.
- Ensuring maintenance on critical equipment is undertaken in such a manner that the system is not off-line due to scheduled maintenance; and,
- Ensuring that when equipment is brought back on-line after scheduled maintenance that all operational specifications are satisfactory.

7.2.4 b) Maintenance of systems, hardware or media containing government information

Information Custodians must consult with Information Owners regarding the value and sensitivity of the information stored on hardware or media when determining whether repairs will be conducted. Information Custodians must ensure that information is safeguarded:

- Maintenance on critical systems must be undertaken in such a manner that the system is not off-line due to scheduled maintenance;
- Hardware or media sent for repairs or maintenance outside of the information processing facility must do so through pre-approved and screened bonded couriers;
- Hardware or media containing confidential or personal information must not have maintenance or repairs conducted off-site;
- Hardware or media containing confidential or personal information that cannot be repaired on-site must be destroyed in accordance with approved disposal standards commensurate with the sensitivity of the information held;
- Maintenance must be factored into system availability requirements; and,
- Repair or maintenance must be conducted within Canada.

Recommended Tests:

Note: ISP 7.2.4 is reported on as part of the annual information security review as CO.7.24.

- Demonstrate that Ministry-specific equipment maintenance logs are up-to-date (e.g., MFD service logs) and/or there is a maintenance schedule maintained, or contracts include scheduled maintenance, and that the maintenance has been conducted.
- Demonstrate that only qualified authorized employees carry out maintenance and repairs in accordance with supplier recommended service intervals and specifications.
- Demonstrate any equipment taken off-site is in a secure state and that no information is vulnerable to loss or unauthorized access.
- Demonstrate service contracts include schedules of regular maintenance activities.
- Demonstrate there a process to ensure the maintenance activities are completed.

7.2.5	**Equipment, information or software belonging to the Province must not be removed from government premises without prior authorization.** **a) Authorized removal of assets**

Purpose: ***To protect assets belonging to the Province from unauthorized removal.***

7.2.5 a) Authorized removal of assets

Information Owners and Information Custodians must establish a formal authorization process for the removal of assets for re-location, loan, maintenance, disposal or any other purpose. Authorization forms for asset removal must include:

- Description and serial numbers;
- Information about where the asset will be located;
- The removal date and return date;
- The identity of the individual responsible for the asset; and,
- Reason for removal of the asset.

The description and serial numbers must be verified when the asset is returned.

Employees must be informed of, and accept responsibility for, protection of the asset (e.g., Terms and Conditions of Use).

Recommended Tests:

Note: ISP 7.2.5 is reported on as part of the annual information security review as CO.7.26.

- Demonstrate the use of authorization forms for asset removal.
- Demonstrate a regular review of equipment inventory check-out and check-in lists matching requests and authorization, purpose (e.g., loan, maintenance), asset information (e.g., serial numbers), current location and custodian contact information.
- Demonstrate employee awareness of controls for removing information assets and acceptance of responsibility.

7.2.6	**Equipment must be protected using documented security controls when off-site from government premises.** **a) Security controls**

Purpose: ***To protect equipment in the custody of employees from loss or unauthorized access.***

7.2.6 a) Security controls

Information Owners and Information Custodians must ensure that equipment being used off-site to access government information is protected commensurate with the sensitivity and the value of the information it contains. Information Custodians must ensure that:

- Sensitive data is encrypted;
- Equipment is protected from unauthorized access by the use of a logical or physical access control mechanism (e.g., password, USB key or smart card);
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and,
- Employees are familiar with operation of the protection technologies in use.

To provide further protection employees must:

- Not leave equipment unattended in a public place;
- Ensure that equipment is under their direct control at all times when travelling;

- Use the physical locking, restraint or security mechanisms provided by the Information Custodian whenever possible;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and,
- Report loss of equipment immediately using the Information Incident Management Process and General Incident or Loss Report (GILR).

Recommended Tests:
Note: ISP 7.2.6 is reported on as part of the annual information security review as CO.7.28.

- Demonstrate in cases of sensitive information that encryption is in place and the device is protected by password or other authentication.
- Demonstrate that employees are made aware of their responsibilities for securing off-site equipment.
- Demonstrate area specific threats are considered prior to authorization for travel outside of Canada.

7.2.7 Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed.
a) Reassignment of hardware and media
b) Destruction of hardware

Purpose: To protect information from unauthorized disclosure.

7.2.7 a) Reassignment of hardware and media
Information Owners must consider the value and sensitivity of the information stored on hardware or media when determining whether it will be reassigned within government or destroyed. Reassignment must only occur within or between government ministries. Prior to reassignment of hardware or media, Information Owners and Information Custodians must ensure:

- The integrity of government records is maintained by adhering to Records Management policies;
- Information and software are erased using methods and standards approved by the Office of the Government Chief Information Officer;
- Roles and responsibilities are documented; and,
- Asset inventories are updated to record details of the erasure and reassignment including:
  - Asset identifier,
  - Date of erasure,
  - Names of employees conducting the erasure,
  - Date of transfer, and,
  - Name of new asset custodian.

Where information is erased by third parties there must be contractual and audit procedures to ensure complete destruction of the media. Third parties must certify that destruction has occurred.

7.2.7 b) Destruction of hardware
Information Owners and Information Custodians are responsible for ensuring hardware media used to store information or software is destroyed in a secure manner. Corporate Information and Records Management Office is responsible for ensuring secure disposal or destruction services are available to Information Owners and Information Custodians.

Guidelines:
A Corporate Supply Arrangement exists for provision of secure media destruction services. Secure destruction service companies must be used to perform media disposal. Contact the Ministry Records Officer for further details.

Recommended Tests:
Note: ISP 7.2.7 is reported on as part of the annual information security review as CO.7.30.

- Demonstrate the ministry, division, or branch maintain records of IT assets sent for disposal.
- Demonstrate that the information classification of assets being disposed is either the highest sensitivity of the information contained within or capable of being processed by the asset.
- Demonstrate that when information is erased by third parties there are contractual and audit procedures to ensure complete destruction of the information.

7.2.8 Employees must ensure unattended equipment has appropriate protection.
a) Protection of unattended equipment

Purpose: ***To reduce risk of unauthorized access, loss or damage to information and information systems.***

7.2.8 a) Protection of unattended equipment
Information Owners must ensure that employees are aware of their responsibilities to secure unattended equipment to prevent unauthorized access to information systems by:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling password protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password protection on mobile devices including portable storage devices; and,
- Being aware of their responsibility to report security weaknesses where the above controls have not been applied.

B.C. Government workstations and other devices used for information system access must automatically activate screen savers or equivalent locking systems after 15 or less minutes of inactivity.

Recommended Tests:
Note: ISP 7.2.8 is reported on as part of the annual information security review as CO.7.32.

- Demonstrate that information systems have a default timeout and are password protected.
- Demonstrate that the requirements to secure unattended equipment are communicated to employees.
- Demonstrate that mobile devices can be wiped remotely.

7.2.9 Employees must ensure the safety of sensitive information from unauthorized access, loss or damage.
a) Securing the work space
b) Secure work habits

Purpose: ***To reduce risk of unauthorized access, loss or damage to information by ensuring employees take reasonable security precautions.***

7.2.9 a) Securing the work space

Employees must secure their work space whenever it is not supervised by an authorized person, including during short breaks, attendance at meetings, and at the end of the work day.

Securing the work space includes:

- Clearing desk tops and work areas;
- Securing documents and mobile or portable storage devices in a locked desk or file cabinet;
- Ensuring outgoing and incoming mail is appropriately secured;
- Enabling a password protected screen saver;
- Shutting down and restarting workstations at the end of each work day;
- Locking doors and windows; and,
- Checking fax machines and printers to ensure that no sensitive information is waiting to be picked up.

7.2.9 b) Secure work habits

Employees must develop and implement security conscious work habits to reduce the likelihood of unauthorized viewing, access or disclosure of sensitive information.

Security conscious work habits include:

- Ensuring sensitive information is protected from accidental viewing by persons passing through the work space;
- Ensuring that only the documents required for current work are out of their normal file cabinet;
- Ensuring white boards, bulletin boards, flip charts do not contain sensitive information when the viewing audience cannot be defined;
- Covering up, filing or storing paper documents when visitors are present in the work area;
- Clearing, changing or turning off the computer screen (e.g., minimize open Windows) so that sensitive information is not displayed when visitors are present in the work area; and,
- Not discussing sensitive information in open work spaces or public areas.

Guidelines:

Ensure that offices can be locked and that storage with locks is available.

Recommended Tests:

Note: ISP 7.2.9 is reported on as part of the annual information security review as CO.7.34.

- Determine if information systems have a default timeout and are password protected.
- Determine information systems are sited in a secure zone that limits access to authorized users.
- Demonstrate employee awareness of responsibilities and requirements to report security weaknesses.

8 Operations Security

This chapter establishes a framework to support the integration of information security in the services provided by government information processing facilities. Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide information services. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve. For critical systems additional requirements are defined in the Critical Systems Standard.

Controls for operations include documented processes, employee duties and formal methods to implement changes to facilities. This includes methods to protect information, create copies for back-up and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

8.1 Operational Procedures and Responsibilities

8.1.1	**Operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented, and maintained.** **a) Operating procedures**

Purpose: ***To ensure correct operations of information systems and information processing facilities.***

8.1.1 a) Operating procedures

Information Custodians must ensure that approved operating procedures and standards are:

- Documented;
- Consistent with government policies, standards and guidelines; and
- Reviewed and updated annually or when there are:
    - Alterations to building layouts,
    - Changes to equipment/systems located in the facility,
    - Changes in business services and the supporting information systems operations, and,
    - As part of any related security incident investigation.

Operations documentation must contain detailed instructions regarding:

- Information processing and handling;
- Last review and update;
- Classification of document;
- System re-start and recovery;
- Back-up and recovery, including on-site and off-site storage;
- Exceptions handling, including a log of exceptions;
- Output and media handling, including secure disposal or destruction;
- Audit and system log management;
- Change management including scheduled maintenance and interdependencies;
- Computer room management and safety;
- Information Incident Management Process;
- Disaster recovery;
- Business continuity; and,
- Operations, technical, emergency and business contacts.

Recommended Tests:

Note: ISP 8.1.1 is reported on as part of the annual information security review as CO.8.4.

- Demonstrate all operational procedures are documented and maintained to current operations.

8.1.2	**Changes to information systems and information processing facilities must be controlled.** **a) Planning changes** **b) Change management process** **c) Implementing change**

Purpose: ***To ensure changes to information systems and facilities are applied correctly and do not compromise the security of information and information systems.***

8.1.2 a) Planning changes

Information Owners and Information Custodians must plan for changes to information systems and information processing facilities by assessing the impact of the proposed change on security by conducting a security review based on the size of the change.

8.1.2 b) Change management process

Information Owners and Information Custodians must plan, document and implement a change management process to control changes by:

- Identifying and recording significant changes;
- Assessing the potential impact, including the security impact, of the change by conducting a Security Threat and Risk Assessment;
- Developing an implementation strategy;
- Obtaining approval of changes from the manager(s) responsible for the information system;
- Planning and testing changes including documenting fallback procedures;
- Communicating change details to relevant employees;
- Identifying the impact on agreements with business partners and third parties including information sharing agreements, Memoranda of Understanding, licencing and provision of services;
- Evaluating that planned changes were performed as intended; and,
- Training technical and operations employees if required.

8.1.2 c) Implementing changes

Information Owners and Information Custodians must implement changes by:

- Notifying affected parties, including business partners and third parties;
- Completing re-certification and re-accreditation as required prior to implementation;
- Training employees if required;
- Documenting and reviewing the documentation throughout the testing and implementation phases;
- Recording all pertinent details regarding the changes; and,
- Checking after the change has been performed that only the intended changes took place.

Recommended Tests:

Note: ISP 8.1.2 is reported on as part of the annual information security review as CO.8.6.

- Demonstrate a change management approval process exists.

- Demonstrate that changes are planned through collaboration with affected parties.
- Demonstrate all procedural documents are updated as part of the change management process.
- Demonstrate that changes are implemented in accordance with an approved change request agreement.
- Demonstrate that a Security Threat and Risk Assessment and Privacy Impact Assessment are part of the change plan process.
- Demonstrate emergency change management capabilities exist to enable a quick and controlled response to resolve an incident(s).

8.1.3 Controls must be applied to limit opportunities for information leakage.
a) Preventing information leakage

Purpose: ***To protect information and information systems from unauthorized access, theft or misuse.***

8.1.3 a) Preventing information leakage

Information Owners and Information Custodians must implement processes to reduce the opportunity for information leakage in information systems by:

- Scanning for malicious code;
- Monitoring resource usage in information systems;
- Identifying and limiting the trusted connections in and out of the government network;
- Controlling third party network connections (e.g., only authorized traffic permitted);
- Using software that is considered to be of high integrity;
- Regular monitoring of information systems; and
- Reviewing usage and access logs for irregularities.

Guidelines:

Scanning outbound media and communications for hidden information should be considered. Canadian Common Criteria Scheme (CCCS) certification may be considered for evaluation of high integrity software.

Recommended Tests:

Note: ISP 8.1.3 is not reported on as part of the annual information security review.

- Demonstrate process controls for mitigating data leakage.
- Demonstrate logs are regularly reviewed for data in transit.

8.1.4 The use of information system resources must be monitored, optimized and projections made of future capacity requirements.
a) Resource capacity management
b) Resource capacity planning

Purpose: ***To reduce the risk of system failures and unacceptable performance levels by monitoring and optimizing resources to meet current and future information system capacity requirements.***

8.1.4 a) Resource capacity management

Information Custodians are responsible for implementing capacity management processes by:

- Documenting capacity requirements and capacity planning processes;
- Identifying and managing storage requirements;
- Including capacity requirements in service agreements;
- Monitoring and optimizing information systems to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
    - New business and information systems requirements,
    - Statistical or historical capacity requirement information, and,
    - Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

8.1.4 b) Resource capacity planning

Information Custodians must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a threat to system security or services. Information Owners and Information Custodians must plan and budget for business and service capacity management.

Guidelines:

Resource capacity management processes should be automated where feasible.

Recommended Tests:

Note: ISP 8.1.4 is reported on as part of the annual information security review as CO.8.8.

- Demonstrate capacity management process is documented and reviewed regularly.
- Demonstrate capacity planning has been completed for critical systems for the projected life of the system (e.g., capital planning, business case).
- Demonstrate information project planning considers additional capacity demand.

8.1.5 Development and test information systems must be separated from operational information systems.
a) Separation requirements

Purpose: ***To reduce the risk of unauthorized or inadvertent changes to operational information systems.***

8.1.5 a) Separation requirements

Information Custodians must protect operational information systems by:

- Separating operational environments from test and development environments (e.g., using different computer rooms, servers, domains and partitions);
- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified employees;
- Preventing access to compilers, editors and other tools from operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems;
- Prohibiting the use of operational data in development, test or training information systems; and,

- Prohibiting the use of personal or sensitive information in development, test or training information systems.

Separating duties between development, test and operational information systems will assist in achieving the separation of systems.

Recommended Tests:
Note: ISP 8.1.5 is reported on as part of the annual information security review as CO.8.10.

- Demonstrate architecture diagrams illustrate clear separation between development, test, production environments and operational systems.
- Demonstrate a Security Threat and Risk Assessment identified the separation and the required controls for development, test, and production environments.
- Demonstrate that a Privacy Impact Assessment has been completed for all systems with personal information.

8.2 Protection from malware

8.2.1	**Security awareness, prevention and detection controls must be utilized to protect information systems against network and host-based threats.** **a) Prevention and detection controls** **b) User awareness**

Purpose: ***To protect the integrity of information systems and software through requirements for the prevention and detection of network and host-based threats.***

8.2.1 a) Prevention and detection controls
Information Custodians must protect government information systems from network and host-based threats by undertaking such activities as:

- Installing, updating and consistently using software designed to scan for, detect and provide protection from network and host-based threats;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malware before use;
- Maintaining business continuity plans to recover from security incidents;
- Regularly reviewing file and data content on critical systems to identify unapproved or unauthorized files and file changes; and
- Scanning back-up media prior to restoration so that malware is not introduced or re-introduced into an information system and network.

The Chief Information Security Officer must ensure processes are implemented to:

- Maintain a critical incident management plan to identify and respond to security incidents; and,
- Maintain a register of specific threat countermeasures (e.g., blocked websites, blocked electronic mail attachment file types, blocked network ports, additional monitoring, etc.) including a description, the rationale, the approval authority and the date applied.

8.2.1 b) User awareness
The Chief Information Security Officer is responsible for developing user awareness programs for threat countermeasures.

Ministry Information Security Officers are responsible for communicating technical advice and providing information and awareness activities regarding network and host-based threats.

Employees are required to complete the information protection courses provided by the Public Service Agency as part of their awareness training.

Recommended Tests:
Note: ISP 8.2.1 is reported on as part of the annual information security review as CO.8.14.

- Demonstrate that devices connecting to government networks have an up-to-date anti-malware solution in place or other similar security measures.
- Demonstrate that employees have been provided with awareness training related to the protection of information (e.g., malware, phishing, spam).

8.3 Backup

8.3.1	**Information and information systems must be backed up and the recovery process tested regularly.** **a) Defining requirements** **b) Safeguarding backup facilities and media** **c) Testing**

Purpose: ***To enable the timely recovery of information and information systems.***

8.3.1 a) Defining requirements
Information Owners and Information Custodians must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems including:

- Confirming that the backup and recovery strategy complies with:
  - Business continuity plans,
  - Policy, legislative, regulatory and other legal obligations, and,
  - Records management requirements, including the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS), and,
- Documenting the backup and recovery processes including:
  - Types of information to be backed up,
  - Schedules for the backup of information and information systems,
  - Backup media management (e.g., retention period, pattern of backup cycles),
  - Methods for performing, validating and labelling backups, and,
  - Methods for validating recovery of the information and information system.

8.3.1 b) Safeguarding backup facilities and media
Information Custodians must conduct a Security Threat and Risk Assessment to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems. Safeguards include:

- Using encryption to protect the backed up information;
- Using digital signatures to protect the integrity of the information;
- Physical and environmental security;

- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and,
- Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.

8.3.1 c) Testing
Information Custodians must regularly test backup and recovery processes.

Recommended Tests:
Note: ISP 8.3.1 is reported on as part of the annual information security review as CO.8.18.

- Demonstrate access controls on backup data.
- Demonstrate that backup media is properly secured commensurate with the information sensitivity (e.g., encryption of personal information).
- Demonstrate backups are stored at a sufficient distance from the main site.
- Demonstrate restoration procedures are documented.
- Demonstrate a successful backup restoration has been completed.

8.4 Logging and monitoring

8.4.1	**Audit logs must be produced, retained and regularly reviewed.** **a) Audit logging** **b) Review of monitoring activities** **c) Audit log retention** **d) Response to alarms**

Purpose: ***To ensure usage of information systems can be monitored and audited.***

8.4.1 a) Audit logging
Information Owners and Information Custodians must ensure that audit logs are used to record user and system activities, exceptions, and information security and operational events including information about activity on networks, applications and systems. Information Owners and Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs.

Audit logs must include, when relevant, the following information:

- User identifier;
- Dates, times and details of key events (e.g., logon and logoff);
- Logon method, location, terminal identity (if possible), network address;
- Records of successful and unsuccessful system logon attempts;
- Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts;
- Changes to system configuration;
- Use of privileges;
- Use of system utilities and applications;

- Files accessed and type of access (e.g., view, read, modify, delete);
- For voice calls: source and destination telephone numbers, date, time, and length of call;
- Name and size of file attachments that are part of or are included in data transmissions (e.g., email, instant messaging, unified communications platforms, etc.);
- Network addresses (source and destination), ports (source and destination), protocols, and transferred network data traffic flow (packets and bytes);
- Alarms raised by the access control system; and,
- Activation and de-activation of protection systems (e.g., anti-virus, intrusion detection).

Audit logs may contain confidential data and access must be restricted to employees with need-to-know privileged access and be protected accordingly. Information Owners and Information Custodians must not have the ability to modify, erase or de-activate logs of their own activities.

If audit logs are not activated, this decision must be documented and include the name and position of the approver, date and a rationale for de-activating the log. Where required, the Privacy Impact Assessment and Security Threat and Risk Assessment must be updated to reflect this decision.

8.4.1 b) Review of monitoring activities

Information Custodians must set up and document processes for the review of audit logs based on the Information Owners assessment of the value and sensitivity of the information assets, the criticality of the system and the resources required for review.

Audit log reviews must:

- Prioritize reviews of high value and highly sensitive information assets;
- Be based on a documented Security Threat and Risk Assessment; and
- Utilize automated tools to identify exceptions (e.g., failed access attempts, unusual activity) and facilitate ongoing analysis and review.

Monitoring must be tested at least annually to ensure that desired events are detected. Analysis of monitoring activities can indicate:

- The efficacy of user awareness and training and indicate new training requirements;
- Vulnerabilities that could be, or that are being, exploited; or
- Increases or decreases in unauthorized access attempts or unauthorized use of privileges.

8.4.1 c) Audit log retention

Audit logs must be:

- Retained according to the approved records retention schedule for the system or information asset; and,
- Retained indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

8.4.1 d) Response to alarms

Information Custodians must establish and document alarm response procedures in collaboration with Information Owners to ensure alarms are responded to immediately and consistently. Information Custodians should have documented authority to shut down all or part of a system or network when the alarm indicates new unacceptable threats are present. When exercising this authority, Information Custodians must report the circumstances to the Information Owners as soon as possible.

Normally, the response to an alarm will include:

- Identification of the alarm event;
- Isolation of the event including affected assets;
- Identification and isolation or neutralization of the source;
- Corrective action;
- Forensic analysis of event;
- Action to prevent recurrence; and,
- Securing of audit logs as evidence.

Recommended Tests:

Note: ISP 8.4.1 is reported on as part of the annual information security review as CO.8.22.

- Demonstrate that information systems audit logs capture the required information.
- Demonstrate logs are retained and reviewed.
- Demonstrate alarms are properly monitored.

8.4.2 Information system logging facilities and log information must be protected against tampering and unauthorized access.
a) Protecting information system logging facilities
b) Protecting log information

Purpose: To preserve the integrity of information system logging facilities and log information.

8.4.2 a) Protecting information system logging facilities

Information Owners are responsible for ensuring periodic independent reviews or audits are conducted to confirm that Information Custodians have implemented appropriate controls.

Information Custodians must implement controls to protect logging facilities and log files from unauthorized modification, access or disposal. Controls must include physical security safeguards such as situating logging facilities within a secure zone with restricted access.

8.4.2 b) Protecting log information

Information Custodians must apply controls to protect log files from tampering or modification. Controls must include:

- Consideration of multi-factor authentication for access to sensitive records;
- Back-up of audit logs to off-site facilities;
- Automatic archiving of audit logs to remain within storage capacity;
- Scheduling the audit logs as part of the records management process; and,
- Digital signing for detecting alteration or corruption where available.

All employees must not have permission to erase logs or de-activate logging of their own activities.

Recommended Tests:

Note: ISP 8.4.2 is reported on as part of the annual information security review as CO.8.24.

- Demonstrate logging information is accurate and meets business needs.
- Demonstrate that the logs are restricted to authorized employees (e.g., access to the logs must be logged).
- Demonstrate that logs are read-only.

8.4.3	**Activities of privileged users must be logged, and the log must be subject to regular independent review.** **a) Activities logged** **b) Independent review**

Purpose: ***To protect government information from unauthorized access, modification or deletion.***

8.4.3 a) Activities logged

Privileged users typically have extensive system permissions not granted to most users. Information Owners and Information Custodians must ensure that the activities of privileged users are regularly reviewed, including logging:

- Event occurrence times;
- Event details, such as files accessed, modified or deleted, errors and corrective action;
- Identity of the account and the privileged user involved; and,
- The system processes involved.

Privileged users must not have permission to erase logs or de-activate logging of their own activities.

8.4.3 b) Independent review

Information Custodians must have a documented process to ensure that activity of privileged users is independently reviewed. Reviews must be conducted regularly and at random with the frequency being commensurate with the criticality, value and sensitivity of system and information assets. Following verification of logs, the individual checking them should digitally sign them and store or archive them securely in accordance with the approved records retention schedule. The audit logs must be reviewed prior to being discarded or overwritten.

Recommended Tests:

Note: ISP 8.4.3 is reported on as part of the annual information security review as CO.8.26.

- Demonstrate privileged user logs are independently reviewed.
- Demonstrate that controls protect against tampering or unauthorized changes to log information.
- Demonstrate logs are reviewed prior to discarding or overwriting.

8.4.4	**Faults must be logged, analyzed and appropriate action taken.** **a) Reporting and logging faults** **b) Analysis, resolution and corrective action**

Purpose: ***To support system security by establishing processes for reporting, logging, analyzing, resolving and correcting system faults.***

8.4.4 a) Reporting and logging faults

Information Owners and Information Custodians must implement processes for monitoring, reporting, logging, analyzing and correcting system faults reported by users and automated detection systems. Fault logging requirements should be determined through a Security Threat and Risk Assessment and Privacy Impact Assessments.

Fault management reports must include:

- Description of fault including date and time, location, extent of fault;

- Analysis of probable source and cause;
- Actions taken to respond to and resolve the fault; and,
- Corrective action taken.

8.4.4 b) Analysis, resolution and corrective action
Information Custodians must review fault logs to ensure that faults have been resolved and documented in a fault management report. Information Custodians must provide the fault management report to Information Owners.

Analysis and corrective action includes:

- Defining the fault and probable cause(s);
- Assessing the effectiveness of corrective action(s);
- Checking to ensure that corrective action has not introduced unforeseen vulnerabilities;
- Identifying trends so that corrective action makes increasingly effective use of resources while improving results;
- Recommending upgrades, replacement of components, software or other elements that create or cause faults;
- Improving fault detection and reporting to reduce the time between fault occurrence and taking corrective action;
- Measuring the exposure caused by the fault;
- Reporting on performance impact(s); and,
- Periodically re-assessing logging requirements.

Recommended Tests:
Note: ISP 8.4.4 is not reported on as part of the annual information security review.

- Demonstrate system faults by Ministry per fiscal year are reported.
- Demonstrate faults that cause information security issues are identified on the annual Information Security Review with an appropriate action plan.
- Demonstrate analysis is being performed in order to identify potentially larger issues (e.g., trend analysis, financial impact).
- Demonstrate logging activities are commensurate with maintaining target level of risk.

8.4.5	**Computer clocks must be synchronized for accurate reporting.** **a) Synchronization** **b) Checking and Verification**

Purpose: ***To ensure the integrity of information system logs.***

8.4.5 a) Synchronization
System administrators must synchronize information system clocks to:

- the local router gateway; or,
- the Government approved clock host.

8.4.5 b) Checking and Verification
System administrators must confirm system clock synchronization:

- Following power outages or brownouts;
- As part of incident analysis and audit log review; and,

- At least semi-annually in conjunction with Daylight Savings Time.

Time discrepancies must be reported to OCIO Helpdesk, Customer Service Centre.
The clock hosts must be synchronized with a national time service such as the Government of Canada, National Research Council's Network Time Protocol server.

Recommended Tests:
Note: ISP 8.4.5 is reported on as part of the annual information security review as CO.8.28.

- Demonstrate system clock synchronization follows the government policies and standards.

8.5 Control of operational software

8.5.1	**The implementation of software on operational information systems providing services must be controlled.** **a) Software changes to operational information systems** **b) Software implementation controls**

Purpose: ***To prevent compromise of operational information systems providing services from unauthorized software installation.***

8.5.1 a) Software changes to operational information systems
Information Owners and Information Custodians must implement procedures to control software installation on operational information systems providing services to ensure that:

- Updates of operational information systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- Operations employees and end users have been notified of the changes, potential impacts and if required have received additional training;
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- Modifications to operational software are logged;
- The number of employees able to perform the updates is restricted and kept to a minimum;
- Development code or compilers are not present on operational information systems; and,
- Vendor supplied software is maintained at the supported level.

8.5.1 b) Software implementation controls:
Pre-Implementation
Before an updated or new information system is implemented into the operational environment, checks must be performed to ensure that:

- A Security Threat and Risk Assessment has been carried out;
- A Privacy Impact Assessment has been performed and approved;
- Limitations of security controls are documented;
- Performance and capacity requirements can be met and support organizations have the capacity to maintain the information system;
- Development problems have been resolved successfully;
- The effects on existing operational information systems are known;
- Arrangements for fall-back have been established if the updated or new information system fails to function as intended;

- Error recovery and restart procedures are established;
- Business continuity plans are developed or updated;
- Operating procedures are tested;
- Changes are communicated to users who may be affected by the change;
- Users are educated to use the information system correctly and securely; and,
- Computer operators and system administrators are trained in how to run the information system correctly and securely.

Implementation
The installation process must include:

- Validating the load or conversion of data files;
- Installing executable code only, and not source code;
- Providing ongoing technical support;
- Implementing new or revised procedures and documentation;
- Discontinuing old software, procedures and documentation;
- Arranging for fall-back in the event of failure;
- Informing the individuals involved of their roles and responsibilities;
- Transferring responsibility for the information system from development teams to operational teams to ensure segregation of duties; and,
- Recording installation activity.

Post-implementation
Post-implementation reviews must include:

- The efficiency, effectiveness and cost of security controls;
- Lessons learned and scope for improvements of security controls; and,
- Security incidents and mitigation.

Recommended Tests:
Note: ISP 8.5.1 is reported on as part of the annual information security review as CO.8.32.

- Demonstrate a Security Threat and Risk Assessment and Privacy Impact Assessment have been completed.
- Demonstrate that the updating of software is implemented by trained administrators only after receiving appropriate authorization from management.
- Demonstrate software is only implemented after exhaustive testing.
- Demonstrate that before any introduction of software to systems, the implementation plan has a rollback strategy.
- Demonstrate an audit log is maintained of all updates and changes to software.

8.5.2 Systems documentation must be protected from unauthorized access.
a) Protection of systems documentation

Purpose: ***To prevent unauthorized access to sensitive information contained in systems documentation.***

8.5.2 a) Protection of systems documentation
Information Custodians and Information Owners must ensure that documented procedures for the secure use and storage of systems documentation are established and followed. Procedures must:

- Require information classification labelling of system documentation;
- Establish lists of users authorized to access system documentation on a 'need to know' basis;
- Establish handling rules for the information regardless of storage media (e.g., electronic, paper);
- Require use of access controls, passwords, encryption or digital signatures as appropriate to the information classification; and,
- Include a compliance monitoring process.

Recommended Tests:

Note: ISP 8.5.2 is not reported on as part of the annual information security review.

- Demonstrate documented procedures for the secure use and storage of systems documentation are followed.

8.6 Technical vulnerability management

8.6.1	**Assessments for known exposures must be conducted to evaluate information system vulnerabilities and the management of associated risks.** **a) Vulnerability response processes**

Purpose: ***To mitigate damage to government operations resulting from exploitation of published vulnerabilities.***

8.6.1 a) Vulnerability response processes

Vulnerabilities which impact government information systems must be addressed in a timely manner to mitigate or minimize the impact on government operations. Information Custodians must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- Monitoring external sources of information on published vulnerabilities;
- Assessing the risk of published vulnerabilities;
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- Applying corrective measures to address the vulnerabilities;
- Completing a Security Threat and Risk Assessment to verify the risk has been mitigated; and,
- Reporting to the Chief Information Security Officer on progress in responding to vulnerabilities.

Responsibilities for vulnerability response by service providers must be included in external party service agreements.

The Chief Information Security Officer must:

- Evaluate vulnerabilities and provide advice on appropriate government responses;
- Monitor progress in responding to vulnerabilities;
- Publish summary reports on vulnerability response activities and costs; and,
- When required, initiate incident response processes to address vulnerabilities.

Recommended Tests:

Note: ISP 8.6.1 is reported on as part of the annual information security review as CO.8.36.

- Demonstrate identified roles and responsibilities are established for the coordination of vulnerability management.
- Demonstrate emergency procedures for high risk vulnerabilities (e.g., Heartbleed, Shellshock) are documented and followed.

- Demonstrate patches are well tested prior to implementation.
- Demonstrate all vulnerability patches are actively logged.
- Demonstrate a priority patching criteria based on risk is established to address the most critical applications and information systems first.

8.6.2 Review of the rules governing the installation of software by employees must be established and implemented.
a) Restrictions on software installation

Purpose: ***To limit the installation of software to authorized employees to avoid security incidents.***

8.6.2 a) Restrictions on software installation

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights. Employees must receive authorization prior to installing software on government devices. Software installation must be consistent with the requirements of the Appropriate Use Policy.

Recommended Tests:

Note: ISP 8.6.2 is reported on as part of the annual information security review as CO.8.38.

- Demonstrate employees are made aware of acceptable/appropriate use policies.

8.7 Information systems audit considerations

8.7.1 Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.
a) Management of information systems compliance checking

Purpose: ***To prevent compliance checking activities from causing unplanned disruptions to operational information systems.***

8.7.1 a) Management of information systems compliance checking

Prior to commencing compliance checking activities such as audits, risk and controls reviews, monitoring or security reviews of operational information systems, the Manager responsible for the compliance checking activity, Information Owners and Information Custodians must define, document and approve the activities by:

- Determining the scope, duration and level of detail of the compliance checking activity;
- Limiting access rights to operational information systems for compliance checking employees to "read only";
- Determining handling requirements for copies of files made by compliance checking employees including:
  - establishing a separate environment for the analysis of files,
  - restricting access to those files,
  - logging the accesses made to those files, and,
  - erasing files at the conclusion of compliance checking activities unless needed to support report findings;

- Identifying special testing or processing which may impact the operational information system (e.g., penetration tests, server vulnerability assessments) and by:
    - notifying the Chief Information Security Officer prior to compliance checking activities to prevent triggering false security alarms from the infrastructure, and,
    - scheduling tests to minimize disruption;
- Submitting the reports of penetration tests or vulnerability assessments to the Chief Information Security Officer immediately upon receipt; and,
- Requiring that employees conducting compliance checking activities maintain a segregation of duty from the operational information systems being checked.

Guidance for compliance checking activities can be obtained from the Information Security Branch, Office of the Government Chief Information Officer.

Recommended Tests:

Note: ISP 8.7.1 is reported on as part of the annual information security review as CO.8.42.

- Demonstrate regular audit requirements timing and scope are agreed upon to minimize disruption.
- Demonstrate there is a clear segregation of duties between the auditor and operational employees.
- Demonstrate all access is monitored and logged.

8.7.2 Access to system audit tools must be controlled to prevent misuse or compromise.
a) Protection of information system audit tools

Purpose: ***To minimize risks to information and information systems from inappropriate use of audit tools.***

8.7.2 a) Protection of information system audit tools

Managers responsible for compliance checking activities and Information Custodians must control the use of audit tools by:

- Restricting access to authorized employees who have a need-to-know;
- Installing or enabling specialized audit tools for the duration required by the compliance checking activity;
- Removing information system access at the conclusion of the compliance checking activities; and,
- Notifying the Chief Information Security Officer prior to the use of audit tools.

Recommended Tests:

Note: ISP 8.7.2 is not reported on as part of the annual information security review.

- Demonstrate the use of audit tools is authorized.

9 Communications Security

This chapter identifies the information security requirements for network and communication services.

9.1 Network security management

9.1.1	**Controls must be implemented to achieve and maintain security within the government network.** **a) Control and management of networks** **b) Configuration control** **c) Secured path** **d) Wireless Local Area Networking** **e) Equipment management** **f) Logging, monitoring and detection** **g) Coordination and consistency of control implementation**

Purpose: ***To ensure that network security controls and network security management practices are implemented and documented to maintain network security.***

9.1.1 a) Control and management of networks

Information Custodians must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached information systems. Selection of controls must be based on a Security Threat and Risk Assessment, taking into account the information security classification determined by the Information Owners, and applicability to the network technology.

The Security Threat and Risk Assessment must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and cryptographic keys;
- Network management information;
- Network pathways and routes;
- Network resources such as bandwidth;
- Network security boundaries and perimeters; and,
- Information system interfaces to networks.

9.1.1 b) Configuration control

To maintain the integrity of networks, Information Custodians must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;

- Access controls and multi-factor authentication;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Status accounting must be regularly performed to ensure that configuration baselines reflect actual device configuration.

9.1.1 c) Secured path

Where required by information classification and a Security Threat and Risk Assessment, information must only be transmitted using a secured path.
Secured paths for information transmission must use controls such as:

- Data, message or session encryption, such as SSH, SSL or VPN tunnels; and,
- Systems to detect tampering.

9.1.1 d) Wireless Local Area Networking

Wireless Local Area Network access points must be authorized by the Office of the Government Chief Information Officer for attachment to the government network. Wireless Local Area Networks must utilize the controls specified by the Chief Information Security Officer and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by government authentication services;
- The use of strong, frequently changed, automatically expiring encryption keys and passwords;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

Where supported by the information classification or a Security Threat and Risk Assessment, additional controls for wireless networks may include:

- Virtual Private Network tunnel technology;
- The use of Desktop Terminal Services (DTS) technology; and,
- Intrusion detection systems, firewalls and Media Access Control (MAC) address filtering.

9.1.1 e) Equipment management

Information Custodians must document responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas.

9.1.1 f) Logging, monitoring and detection

To facilitate monitoring, response and investigation, logging to a centralized log management service must be enabled, including logging of:

- Traffic traversing network security boundaries;
- Traffic within networks housing sensitive or critical systems or information;
- Security-relevant events on network devices, such as operator logon and configuration changes; and,
- Security-relevant events on systems that provide authentication and authorization services to network infrastructure devices such as routers, firewalls or switches.

Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g., automation of log monitoring and event alerting). Logs from available sources (including, but not limited to, network traffic, network firewalls, Intrusion Prevention Systems, routers, switches, content filtering, servers, applications, databases, application firewalls, authentication services) must be continuously correlated to enable detection and response to security events and intrusions, that otherwise would go undetected without such correlation and alerting.

In order to support the monitoring and correlation of logs from available sources, in cases when infrastructure or services are provided via a third-party, it must be ensured that security event logs from the respective outsourced infrastructure or services can be forwarded real-time to the government centralized monitoring services to allow for the centralized monitoring, correlation and alerting across government.

Information Custodians must ensure there is a clear segregation of duties for employees involved in logging, monitoring or detection activities. Active automated surveillance of networks must be implemented to detect and report on security events (e.g., network intrusion detection systems). Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information systems as determined by a Security Threat and Risk Assessment.

9.1.1 g) Coordination and consistency of control implementation

Information Owners and Information Custodians must document network security controls in the System Security Plan including:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Roles and responsibilities for network security management;
- Specific procedures and standards used to mitigate risks and protect the network;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures (including monitoring frequency, review and remediation processes).

Recommended Tests:

Note: ISP 9.1.1 is reported on as part of the annual information security review as CO.9.4.

- Demonstrate that access to the network devices is restricted and is done via central authentication and automated updates.
- Demonstrate configuration controls are established to safeguard the confidentiality and integrity of data passing across networks.
- Demonstrate controls for wireless local area networks meet the standard requirements.
- Demonstrate that network activities are monitored and logged.

9.1.2 Security configuration, service levels and management requirements of all network services must be documented and included in any network service agreement.
a) Network service agreement

Purpose: To specify what security features are required for delivery of a network service.

9.1.2 a) Network service agreement

Formal network service agreements must be established between network service providers and consumers of network services to specify service levels, services offered, security requirements and security features of network services. The network service agreement must include specification of:

- The rules of use to be followed by consumers to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed;
- Security incident response responsibilities, contacts and procedures; and,
- The requirement to meet or exceed government Information Security Policy and standards.

Information Owners and Information Custodians must confirm that the specified security features are implemented prior to commencement of service delivery.

Recommended Tests:

Note: ISP 9.1.2 is reported on as part of the annual information security review as CO.9.6.

- Demonstrate configuration controls are established to safeguard the confidentiality and integrity of data passing across government networks.
- Demonstrate the requirement for Security Threat and Risk Assessment is included in service level agreements for all networks.
- Demonstrate all network service arrangements have a documented network service agreement in place that specifies security features.
- Demonstrate network service provider's security controls are regularly monitored and have annual audits completed.

9.1.3 Groups of information services, users and information systems must be segregated on networks.
a) Segregation based on risk and requirements

Purpose: ***To isolate information systems, users and networks based on risk and business connectivity requirements.***

9.1.3 a) Segregation based on risk and requirements

Information Custodians must segregate services, information systems and users to support business requirements for information system connectivity and access control based on the principles of least privilege, management of risk and segregation of duties.

Information Custodians must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

The techniques and technologies selected for network segregation must be based on Security Threat and Risk Assessment and Privacy Impact Assessment findings. Factors to consider include:

- The information and information system security classification;
- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks, and sensitivity to eavesdropping (e.g., the Internet is a less trusted network than a controlled server network zone);

- Transparency, usability and management costs of network segregation technologies; and,
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

Network zones must be defined and network perimeters established, according to business requirements and risk as identified in the Security Threat and Risk Assessment and Privacy Impact Assessment (e.g., network zones for public access, Ministry, core network, wireless network). Information system operational management and business applications must be defined and separated by network flow control points.

Guidelines:
Security gateways should be used to verify the trustworthiness of devices attempting to connect to the network (e.g., VPN Quarantine systems, network switch isolation and admission control systems).

Recommended Tests:
Note: ISP 9.1.3 is reported on as part of the annual information security review as CO.9.8.

- Demonstrate that access to the network by devices is restricted and is done via central authentication and automated updates.
- Demonstrate configuration controls are established to safeguard the confidentiality and integrity of data passing across public networks.
- Demonstrate configuration controls for wireless local area networks.
- Demonstrate appropriate security monitoring and logging of network activities.

9.1.4	**Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system.** **a) Network address control** **b) Control of routing information**

Purpose: ***To control network routing to prevent unauthorized access or bypassing of security control points.***

9.1.4 a) Network address control
Information Custodians must implement mechanisms to prevent network address spoofing and routing of spoofed network traffic (e.g., through use of router access control lists).
Security gateways must be considered for network access control points, in accordance with information system security classification requirements. Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

9.1.4 b) Control of routing information
Information Custodians must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).

Recommended Tests:
Note: ISP 9.1.4 is not reported on as part of the annual information security review.

- Demonstrate Information Security Threat and Risk Assessments are completed on all devices that provide network routing.

9.2 Information transfer

9.2.1	**Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information through all types of electronic communication services.** **a) Electronic information exchange**

Purpose: ***To protect information from unauthorized disclosure.***

9.2.1 a) Electronic information exchange

The Chief Information Security Officer must document and implement procedures to protect information from interception, copying, misrouting and disposal when being transmitted electronically. Transmission methods include but are not limited to:

- E-mail, including attachments;
- Electronic file transfer (e.g., File Transfer Protocol (FTP), Electronic Data Interchange (EDI));
- Use of mobile devices;
- Telephone, cell, and other voice messaging;
- Faxes; and,
- Instant messaging.

Recommended Tests:

Note: ISP 9.2.1 is reported on as part of the annual information security review as CO.9.12.

- Demonstrate the procedures designed to protect transferred information from interception, copying, modification, misrouting and disposal are in place.
- Demonstrate controls for detection and protection against malware are in place.
- Demonstrate employees are provided with training on recognizing phishing attempts.
- Demonstrate employees are provided with training for information exchange policies, procedures and controls.
- Demonstrate employees are provided with training on procedures for protecting information from unauthorized disclosure.

9.2.2	**Information and software exchange agreements between the Province and other organizations must address the secure transfer of information between parties.** **a) Exchange agreements** **b) Information and software exchange requirements**

Purpose: ***To protect information or software from loss or unauthorized disclosure.***

9.2.2 a) Exchange agreements

Information Owners and Information Custodians must ensure the terms and conditions for secure exchange of information assets with external parties is documented in an agreement. The agreement must define:

- Custody and control accountabilities;
- Authority of a custodian to publish, grant access to or redistribute the information;

- Purpose and authorized uses of the information or software;
- Limitations on data linkage;
- Duration, renewal and termination provisions;
- Primary contacts for agreement, governance and management;
- Requirements for:
    - Protecting information according to its security classification,
    - Handling information (e.g., recording authorised recipients, confirming receipt of transmitted data, periodically reviewing records of authorised recipients),
    - Labelling information (e.g., methods to be used to apply and recognize labelling),
    - Maintaining integrity and non-repudiation of information, and,
    - Media management and disposal;
- Technical standards for transmission, recording or reading information or software;
- Responsibilities for reporting privacy and security incidents and breaches;
- Liability, accountability and mitigation strategies, for attempted, suspected or actual privacy and security incidents and breaches; and,
- Problem resolution and escalation processes.

9.2.2 b) Information and software exchange requirements
Information Owners and Information Custodians must ensure an approved Privacy Impact Assessment and a Security Threat and Risk Assessment are completed for the information or software covered by the exchange agreement.

Exchange agreements must be reviewed by legal counsel for the Province prior to being signed.

Guidelines:
Province of B.C. Legal Services should be consulted during the development of sharing agreements.

Recommended Tests:
Note: ISP 9.2.2 is reported on as part of the annual information security review as CO.9.14.

- Demonstrate that exchange of information with external parties is covered by an information sharing agreement.
- Demonstrate Security Threat and Risk Assessments are completed on all information sharing agreements assessing the transfers of information.
- Demonstrate Privacy Impact Assessments are completed on all information sharing agreements.
- Demonstrate that information and software exchange agreements with external parties have been reviewed by Legal Services.

9.2.3 Information transmitted by electronic messaging must be appropriately protected.
a) General requirements
b) Custody of electronic messages

Purpose: To enable secure and trustworthy electronic messaging

9.2.3 a) General requirements
Electronic messaging services must be managed to protect the integrity of government messages by:

- Protecting messages from unauthorized access, modification or denial of service;
- Ensuring correct addressing and transportation of messages;

- Providing reliable and available messaging infrastructure; and,
- Conforming to legislative, regulatory and policy requirements.

The Government Chief Information Officer must approve implementation of, and significant modification to, electronic messaging systems.

Employees must support the responsible use of electronic messaging services by:

- Using only government electronic messaging systems for conducting government business, including systems for remote access to government messaging systems from publicly available networks;
- Using only authorized encryption for e-mail or attachments;
- Not automatically forwarding government e-mail to external e-mail addresses; and,
- Maintaining the confidentiality and privacy of information being communicated in electronic messages as appropriate to the sensitivity and classification of the information.

Information Owners must authorize and approve the use of social media services and other non-government electronic messaging services for conducting government business.

9.2.3 b) Custody of electronic messages

Electronic messages created, compiled, sent or received on government information systems are records of the government. These records:

- Are the property of the Government of British Columbia;
- Must be managed in accordance with the Information Management Act and related regulations, policies, standards and procedures; and,
- Are subject to the access and the protection of privacy provisions of the Freedom of Information and Protection of Privacy Act.

Recommended Tests:

Note: ISP 9.2.3 is reported on as part of the annual information security review as CO.9.16.

- Demonstrate that employees are aware that electronic information on government systems constitutes a government record.
- Demonstrate that employees are aware of the secure electronic messaging requirements.
- Demonstrate information security classification and labeling is used to identify protection requirements.
- Demonstrate consideration for record management is given when using electronic messaging.
- Demonstrate a Security Threat and Risk Assessment and a Privacy Impact Assessment is completed on all electronic messaging services.

9.2.4 Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems.
a) Information in business information systems
b) Shared directories

Purpose: To restrict access to information in shared business information systems.

9.2.4 a) Information in business information systems

Information Owners must document and implement procedures to restrict access to information in interconnected internal administrative and productivity information systems that support government such as e-mail, calendars and financial systems.

A Security Threat and Risk Assessment must be conducted to:

- Determine if business information systems provide sufficient protection for the information being shared;
- Define controls to manage information sharing;
- Reduce the risk of social engineering; and,
- Identify access control requirements.

9.2.4 b) Shared directories

The status of employees must be indicated in shared directories (e.g., employee or contractor).

Recommended Tests:

Note: ISP 9.2.4 is not reported on as part of the annual information security review.

- Demonstrate that a Security Threat and Risk Assessment has been completed.

9.2.5 A confidentiality agreement reflecting organizational requirements for the handling of information must be in place and reviewed regularly.
a) Confidentiality agreements

Purpose: ***To ensure employees understand their role in maintaining the confidentiality of information and information systems.***

9.2.5 a) Confidentiality agreements

Information Owners and Information Custodians must:

- Ensure employees are informed of their obligation to maintain the confidentiality of information; and,
- Ensure individuals other than employees accept and sign an agreement to maintain the confidentiality of information.

Confidentiality requirements must be reviewed and updated annually.

Recommended Tests:

Note: ISP 9.2.5 is reported on as part of the annual information security review as CO.9.18.

- Demonstrate that a Ministry on-boarding process includes confidentiality agreements.
- Demonstrate that employees are made aware of the requirements to keep confidential information safe from disclosure.

10 System Acquisition, Development and Maintenance

This chapter establishes requirements for incorporating security measures into the life-cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

10.1 Security requirements of information systems

10.1.1	**Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.** **a) Security requirements for information systems** **b) Security requirements at implementation**

Purpose: ***To integrate system security requirements into business processes supporting the development, maintenance and acquisition of information systems.***

10.1.1 a) Security requirements for information systems

Information Owners must conduct a Security Threat and Risk Assessment and a Privacy Impact Assessment during the requirements phase when developing, implementing major changes to, or acquiring an information system, to:

- Identify the security requirements necessary to protect the information system; and,
- Assign a security classification to the information and the information system.

The Information Owner must ensure that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures which include:

- Testing the information system to verify that it functions as intended;
- Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses; and,
- Using common government processes and services (e.g., authentication, access control, financial management).

10.1.1 b) Security requirements at implementation

Information Owners and Information Custodians must ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. Prior to implementation, information systems must be assessed to verify the adequacy of, and document the details of, the security controls used, by completing a security certification.

Different tiers of applications need to be separated across different platforms or servers (e.g., web interface must be on a different server from the data base).

Information systems should have a documented and maintained System Security Plan. The Plan should include:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Results of the system certification;
- Roles and responsibilities for information system security management;
- Specific procedures and standards used to mitigate risks and protect the information system;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures.

While Security Threat and Risk Assessments are not required for all apps on mobile devices, where the app is used for processing government information, a Security Threat and Risk Assessment and Privacy Impact Assessment must be completed before the use of the app. Apps should be downloaded only from official vendor provided app stores. Mobile devices attached to the government network must be used according to vendor specifications (e.g., not removing vendor built-in restrictions).

Employees should always consider potential risks before downloading apps on their mobile devices. Some apps have been found to have harmful effects and may inadvertently release information from the mobile device to third parties.

Recommended Tests:

Note: ISP 10.1.1 is reported on as part of the annual information security review as CO.10.4.

- Demonstrate information security requirements are derived from compliance requirements in information security policies, guidelines and regulations.
- Demonstrate a Privacy Impact Assessment has been completed for all information systems with personal information.
- Demonstrate users and operators have a clear understanding of roles and responsibilities.

10.1.2 Information in application services information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.
a) Electronic commerce
b) Electronic documents

Purpose: To enable secure electronic commerce for the delivery of government services.

10.1.2 a) Electronic commerce

Prior to initiating or implementing electronic commerce information systems, Information Owners and Information Custodians must:

- Ensure that the Security Threat and Risk Assessment is conducted and addresses threats and risks related to electronic commerce;
- Confirm that a Privacy Impact Assessment has been conducted and approved;
- Determine the security classification of the information and information system(s) involved;
- Ensure that the user notification and acceptance of terms and conditions of use complies with government policies and standards;
- Ensure multi-factor authentication is used commensurate with the sensitivity and value of the information;
- Develop and implement processes to maintain content currency;
- Confirm the information system has received security certification and accreditation; and,

- Develop Business Continuity Plans and supporting Disaster Recovery Plans.

10.1.2 b) Electronic documents
When accepting or submitting electronic documents, Information Owners and Information Custodians must:

- Authenticate the users claimed identity;
- Determine an authorization process for approving contents, issue or sign key documents;
- Determine the requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the confidentiality of contracts; and,
- Ensure the protection requirements of any confidential information.

Recommended Tests:
Note: ISP 10.1.2 is reported on as part of the annual information security review as CO.10.6.

- Demonstrate applied authorization and authentication when providing services over networks.
- Demonstrate the level of protection for payments (e.g., Payment Card Industry standards).
- Demonstrate procedures for ensuring confidentiality.

10.1.3 Information systems utilizing on-line transactions must have security controls commensurate with the value and sensitivity of the information.
a) On-line transaction security
b) Payment card transaction security

Purpose: ***To maintain the confidentiality, integrity and availability of on-line transactions in information systems.***

10.1.3 a) On-line transaction security
Information Owners and Information Custodians are responsible for ensuring information systems containing on-line transactions have implemented security controls commensurate with the value and sensitivity of the information.

Security controls must be implemented to prevent incomplete transmission, misrouting, repudiation of transaction, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

10.1.3 b) Payment card transaction security
Information Owners and Information Custodians are responsible for ensuring that information systems used for processing payment card transactions, or connected to payment card transaction processing systems, comply with the Payment Card Industry Data Security Standard.
The Payment Card Industry Data Security Standard V3.0 has 12 high-level requirements:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;
- Protect stored cardholder data;

- Encrypt transmission of cardholder data across open, public networks;
- Protect all systems against malware and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;
- Restrict access to cardholder data by business need-to-know;
- Identify and authenticate access to system components;
- Restrict physical access to cardholder data;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and,
- Maintain a policy that addresses information security for all employees.

Recommended Tests:

Note: ISP 10.1.3 is reported on as part of the annual information security review as CO.10.8.

- Demonstrate that storage of transaction details is located outside any publicly accessible environment.
- Demonstrate security controls are commensurate with the classification of the information that is being protected.

10.2 Security in development and support process

10.2.1	**Policies, standards, and guidelines for the development of software and systems must be established and applied to developments within the organization.** **a) Secure development process** **b) Secure programming techniques**

Purpose: ***To ensure that information security is designed and implemented within the development life-cycle of information systems.***

10.2.1 a) Secure development process

Information Owners and Information Custodians must ensure that software and systems developed internally follow established policies, standards and best practices for secure development process. The established policies and standards must be applied consistently to all developments within the organization.

A secure development process is a necessity in developing a secure information system. Within a secure development life-cycle of information systems, the following aspects must be considered:

- Security of the development environment;
- Security in the software development methodology;
- Secure coding guidelines for each programming language used;
- Inclusion of security requirements starting from the design phase;
- Security checkpoints within the development milestones;
- Secure repositories;
- Security in the version control and updates;
- Required application security knowledge; and,
- Developer capability of avoiding, finding and fixing vulnerabilities.

10.2.1 b) Secure programming techniques

Secure programming techniques must be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or are not consistent with current best practices. Secure coding standards must be considered and where relevant mandated for use.

- Program code must not be altered unless authorized to do so;
- Any variations to program code must be documented; and,
- All changes to existing code must ensure applicable standards have been applied for program security.

If development is outsourced, the organization must obtain assurance that the external party complies with the policies for secure development.

Recommended Tests:

Note: ISP 10.2.1 is reported on as part of the annual information security review as CO.10.12.

- Demonstrate security requirements were defined in the design phase.
- Demonstrate security in version control.
- Demonstrate developer capability in identifying and addressing vulnerabilities.
- Demonstrate a Privacy Impact Assessment has been completed for all software.

10.2.2 Changes to software must be controlled by the use of formal change control procedures.
a) Changes to software during information systems development
b) Changes to software for operational information systems

Purpose: To ensure that information systems are not compromised from changes to software.

10.2.2 a) Changes to software during information systems development

Information Owners must implement a change control process during development which includes:

- Requiring that change requests originate from authorized employees;
- Requiring that proposed changes are reviewed and assessed for impact; and,
- Logging all requests for change.

10.2.2 b) Changes to software for operational information systems

Information Owners must implement a change control process during the maintenance phase including:

- Requiring that change requests originate from authorized employees;
- Performing an impact assessment considering items such as the System Security Plan and proposed modifications;
- Documenting fallback plans;
- Documenting approval of changes proposed prior to the commencement of the work;
- Documenting the acceptance tests and approval of the results of acceptance testing;
- Updating the System Security Plan and other system, operations and user documentation with the details of changes in accordance with records management policy;
- Maintaining version control for all changes to the software; and,
- Logging all requests for change.

Recommended Tests:

Note: ISP 10.2.2 is reported on as part of the annual information security review as CO.10.14.

- Demonstrate there is an authorization process and scheduled procedures are followed.
- Demonstrate all software is thoroughly tested prior to implementation.

- Demonstrate that there was a change control procedure for changes to the application(s) that included a means to back-out, changes were pre-approved and authorized, and all documentation has been properly updated.
- Demonstrate there is a version control for all software updates.

10.2.3 Information systems must be reviewed and tested when operating system changes occur.
a) Changes to the operating system

Purpose: To ensure information systems will not be disrupted or compromised.

10.2.3 a) Changes to the operating system

Information Custodians must notify information system Information Owners and other affected parties of operating system changes to allow:

- Sufficient time for the review and testing of information systems prior to implementation;
- Review of System Security Plans to ensure information systems will not be compromised by the change;
- Significant changes to the operating system must have a completed Security Threat and Risk Assessment completed;
- Information system testing with the changes to the operating system in a separate (i.e., test) environment; and,
- Update of business continuity plans if required.

Recommended Tests:

Note: ISP 10.2.3 is reported on as part of the annual information security review as CO.10.16.

- Demonstrate application control and integrity procedures to ensure that security has not been compromised by changes to the platform.
- Demonstrate that notification of platform changes permit adequate time for appropriate testing prior to implementation.
- Demonstrate the business continuity plan has been updated to reflect platform changes.
- Demonstrate platforms with personal information processing have a completed Privacy Impact Assessment.

10.2.4 Modification of commercial-off-the-shelf software is limited to essential changes that are strictly controlled and documented.
a) Modifying commercial-off-the-shelf software
b) Applying vendor supplied patches and updates

Purpose: To reduce the risk of information system functionality loss.

10.2.4 a) Modifying commercial-off-the-shelf software

Other than vendor supplied patches, commercial-off-the-shelf (COTS) software must not be modified except in exceptional circumstances when needed for a critical business requirement. This requirement must be documented and approved by the Information Owner and Information Custodian.

If changes to COTS software are required, the Information Owners and Information Custodians must determine:

- The effect the change will have on the security controls in the software;
- If consent of the vendor is required;

- If the required functionality is included in a new version of the software;
- If government will become responsible for maintenance of the software as a result of the change; and,
- Compatibility with other software in use.

If changes are made to COTS software the original software must be kept unaltered and the changes must be:

- Logged and documented, including a detailed technical description;
- Applied to a copy of the original software; and,
- Tested and reviewed to ensure that the modified software continues to operate as intended.

10.2.4 b) Applying vendor supplied patches and updates

A software update management process must be maintained for commercial-off-the-shelf (COTS) software to ensure:

- The most up-to-date approved patches have been applied; and,
- The version of software is vendor supported.

Recommended Tests:

Note: ISP 10.2.4 is reported on as part of the annual information security review as CO.10.18.

- Demonstrate a copy of the unmodified software is retained.
- Demonstrate a software management program is in place to ensure software patching is up-to-date.
- Demonstrate all changes to software are thoroughly tested prior to implementation.

10.2.5 Principles for engineering secure systems must be established, documented, maintained and applied to any information system implementation efforts.
a) Secure engineering principles
b) Outsourcing engineering security
c) Application development

Purpose: ***To ensure information security is designed in all architectural layers of information systems.***

10.2.5 a) Secure engineering principles

Information Owners and Information Custodians must establish and document secure information system engineering procedures based on security engineering principles and best practices. The procedures must be applied to all in-house information system engineering activities. Security must be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology must be analyzed for security risks and the design must be reviewed against known attack patterns.

Secure engineering procedures must be reviewed regularly to ensure they remain current to reflect the changes in the environment and threat landscape.

10.2.5 b) Outsourcing engineering security

Information Owners and Information Custodians must ensure that contracts and other binding agreements incorporate the secure engineering principles and procedures for outsourced information systems.

10.2.5 c) Application development
Application development procedures must apply secure engineering techniques in the development of applications that have input and output interfaces and provide guidance on user authentication techniques, secure session control and data validation, sanitization and elimination of debugging codes.

Recommended Tests:
Note: ISP 10.2.5 is reported on as part of the annual information security review as CO.10.20.

- Demonstrate information systems engineering is based on security engineering principles that are documented and are applied.
- Demonstrate new technologies are analyzed for security risks.
- Demonstrate new technology designs are reviewed against known attack patterns.

10.2.6 Organizations must establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life-cycle.
a) Secure development environment

Purpose: ***To ensure the security of information during the development and system integration process.***

10.2.6 a) Secure development environment
A secure development environment includes people, processes and technologies associated with system development and integration. Information Owners and Information Custodians must assess the risks associated with individual system development efforts and establish secure development environments for system development, considering:

- Sensitivity of data to be processed, stored or transmitted by the system;
- Applicable external and internal requirements (e.g., from regulations, policies and standards);
- The need for segregation between different development environments;
- Security controls already in place that support system development;
- Trustworthiness of employees working in the environment;
- The degree of outsourcing associated with system development;
- Control of access to the development environment;
- Monitoring of changes to the environment and code stored therein;
- Backups are stored at secure offsite locations; and,
- Control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, Information Owners and Information Custodians must document corresponding processes in secure development procedures and provide these to all individuals who need them.

Personal information must not be used in the testing or development phases without a valid policy exemption from the Office of the Chief Information Officer.

Recommended Tests:

Note: ISP 10.2.6 is reported on as part of the annual information security review as CO.10.22.

- Demonstrate that all applicable regulations and standards are considered in the development phase.
- Demonstrate segregation between development, test and operational environments.
- Demonstrate that security is considered throughout each step of the system development life-cycle.
- Demonstrate employees involved with the systems development are made aware of system development security.

10.2.7 Controls must be applied to secure outsourced information system development.
a) Outsourced information system development

Purpose: To ensure information systems perform as expected and meet security requirements.

10.2.7 a) Outsourced information system development

Information Owners and Information Custodians must consider the following when outsourcing information system development:

- Procurement policy for licencing, ownership and intellectual property rights;
- Escrow arrangements in the event of the failure of the external party;
- Testing of the information system for common vulnerabilities and malicious code;
- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information system.

Information Owners and Information Custodians must ensure that the outsourced information system meets the requirements defined in the system development agreements.

Recommended Tests:

Note: ISP 10.2.7 is reported on as part of the annual information security review as CO.10.24.

- Demonstrate identification of ownership in outsourcing software development.
- Demonstrate that intellectual property rights are managed through licencing agreements.
- Demonstrate audit access is stipulated in procurement contracts.
- Demonstrate information system security is involved in every step of outsourced development.

10.2.8 Testing of security functionality must be carried out during development.
a) Testing during development

Purpose: To ensure that security functionality is carried out during the development process.

10.2.8 a) Testing during development

Information Owners and Information Custodians must ensure that new and updated systems undergo thorough testing and verification during the development processes. A detailed schedule of test activities, inputs and expected outputs under a range of conditions must be prepared as part of testing and verification processes.

Independent acceptance testing must be undertaken to ensure that the system works as expected and only as expected. The extent of testing must be in proportion to the importance and nature of the system.

Recommended Tests:
Note: ISP 10.2.8 is reported on as part of the annual information security review as CO.10.26.

- Demonstrate all new and updated systems are tested prior to implementation.
- Demonstrate acceptance testing is segregated from development.

10.2.9 Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.
a) System acceptance process
b) System acceptance criteria
c) Security certification
d) System accreditation

Purpose: ***To ensure that new or upgraded information systems are tested against defined, agreed and documented criteria for acceptance, prior to becoming operational.***

10.2.9 a) System acceptance process
Information Owners must ensure that system acceptance criteria are defined as part of the system development and acquisition process.

Prior to implementing new or upgraded information systems, Information Owners and Information Custodians must ensure:

- Acceptance criteria are identified including privacy, security, systems development and user acceptance testing;
- Security certification is attained, indicating the system meets minimum acceptance criteria; and,
- Security accreditation to proceed with implementation is attained.

A Privacy Impact Assessment must be completed for new or upgraded information systems.

10.2.9 b) System acceptance criteria
Information Owners and Information Custodians must document system acceptance criteria, including:

- Projected performance and resource capacity requirements;
- Disaster recovery, restart, and contingency plans and procedures;
- Impact on standardized routine operating procedures and manual procedures;
- Implementation of security controls;
- Assurance that installation of the new system will not adversely affect existing systems, particularly at peak processing times;
- Business continuity arrangements;
- Training requirements; and,
- User acceptance testing.

10.2.9 c) Security certification
The Information Owners and Information Custodians must receive assurance that a new or updated information system meets minimum security acceptance criteria.

Assurance should be obtained by conducting either an independent Security Threat and Risk Assessment or a Risk and Controls Review which determines whether a system includes adequate controls to mitigate security risks. This process will also determine the effect of the new system on the overall security of government information systems.

10.2.9 d) System accreditation
Information Owners and Information Custodians must authorize the implementation of new or upgraded information systems based on the degree to which the acceptance criteria are satisfied.

Recommended Tests:
Note: ISP 10.2.9 is reported on as part of the annual information security review as CO.10.26.

- Demonstrate that the criteria for acceptance are identified during the procurement phase.
- Demonstrate Privacy Impact Assessments are completed prior to acceptance.
- Demonstrate that all acceptance tests are documented.

10.3 Correct processing in applications

10.3.1 Data input to an information system must be validated to ensure that it is correct and appropriate.
a) Input data validation

Purpose: ***To maintain the integrity of information in information systems by preventing the introduction of invalid or incomplete data.***

10.3.1 a) Input data validation
Information Owners must ensure the validity and integrity of data input to information systems by:

- Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits);
- Checking for invalid characters in data fields;
- Making key fields mandatory;
- Verifying the plausibility of input data using business rules;
- Protecting against common attacks (e.g., buffer overflows); and,
- Using control balances to verify complete input and processing.

10.3.2 Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity.
a) Internal processing

Purpose: ***To prevent errors, loss, unauthorized modification or misuse of information in information systems.***

10.3.2 a) Internal processing
Information Owners must require that information systems include internal processing checks to:

- Detect unauthorized or incorrect changes to information;
- Prevent information from being accidentally overwritten;
- Prevent internal information from being disclosed via information system responses;
- Protect against common attacks (e.g., buffer overflows);

- Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers;
- Maintain audit trails; and,
- Provide error and exception reports.

Information Owners must ensure that error and exception reports are monitored, followed up and signed off on a regular basis.

10.3.3 Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content.
a) Message integrity

Purpose: ***To prevent errors, loss, unauthorized modification or misuse of information in information systems.***

10.3.3 a) Message integrity
Information Owners must determine message integrity requirements during the requirements definition phase of system development or acquisition.

10.3.4 Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
a) Output data validation

Purpose: ***To verify correct information processing for output data.***

10.3.4 a) Output data validation
Information Owners must require that processes are documented to validate the data output from an information system by:

- Reconciling control balances to verify that data is processed accurately;
- Verifying the plausibility of output data using business rules;
- Providing sufficient information for a reader or subsequent information system to determine the accuracy, completeness, precision and classification of the information;
- Maintaining audit trails; and,
- Providing error and exception reports.

Information Owners must ensure that error and exception reports are monitored, followed up and signed off on a regular basis.

10.4 Test data

10.4.1 Test data must be protected and controlled using the same procedures as for data from operational information systems.
a) Protection of test data

Purpose: ***To protect information from unauthorized access or use.***

10.4.1 a) Protection of test data

Information Owners must implement procedures to ensure that:

- Using test data extracted from operational information systems is authorized and logged to provide an audit trail;
- Test data is protected with controls appropriate to the security classification of the information and information system; and,
- Data from operational information systems is removed from the test environment once testing is complete.

Sensitive or personal information from operational information systems should not be used as test data. Where personal or sensitive data must be used for testing purposes, sensitive details and content should be removed, depersonalized or de-identified.

In rare cases when sensitive or personal data from operational systems has to be used for testing purposes, the following conditions must be met:

- Information Owners must provide a strong business case for the use of operational data containing sensitive or personal data for testing purposes;
- Privacy Impact Assessment and Security Threat and Risk Assessment must be completed specific to the use of operational data in test;
- Use of production data for testing purposes must be approved by the program area Executive Director and Ministry Chief Information Officer;
- Testing with the use of operational data must occur only in a production-like environment;
- The data to be used for testing purposes in the production-like environment must be handled with the same care and diligence as in the production environment with the same or more stringent security controls;
- Access to test data must be limited to the minimum number of individuals required to perform testing activities and must be based on clearly defined roles and responsibilities, and formal approval process;
- Information Owners must ensure that access to sensitive or personal information used for testing is monitored and reviewed on a regular basis to detect inappropriate or unauthorized access attempts, at a minimum once a week;
- Where sensitive or personal information is used, Information Owners must ensure that only information fields necessary for testing be used (e.g., if successful results can be achieved using the last four digits of a Social Insurance Number, avoid using the whole number);
- Information Owners must ensure that the smallest subset of sensitive or personal information is used, which is necessary to complete the testing (e.g., if successful results can be achieved using a small number of records, avoid using the whole dataset);
- After testing activities are completed, Information Owners must ensure that test data is erased from the production-like environment in accordance with government standards;
- Information Owners must maintain detailed project documentation on testing activities and processes for audit purposes, including a list of employees involved in testing, date and time when testing began and ended, any deviations from the established processes or procedures that may affect the existing security controls, and any other relevant information; and,
- The documentation must demonstrate why the use of sensitive or personal information is necessary.

Information Owners must ensure that the use of personal information for testing purposes does not contravene the requirements of the Freedom of Information and Protection of Privacy Act. Privacy,

Compliance and Training Branch in the Ministry of Finance manages privacy for the Province and should be consulted when test data involves personal information.

Guidelines:
Output from test systems should be labelled “test”.

Recommended Tests:
Note: ISP 10.4.1 is reported on as part of the annual information security review as CO.10.32.

- Demonstrate that testing requires production data and cannot be done reliably otherwise.
- Demonstrate controls applied to test data are appropriate for the security classification of the information or the information system.
- Demonstrate personal or sensitive data is depersonalised or removed prior to its use in test, unless it is required.
- Demonstrate evidence of authorization approvals for use of operational data in test systems.
- Demonstrate architecture documentation that details what access controls exist on test systems.

11 Supplier Relationships

This chapter covers the requirements for information security in supplier agreements. These are important to consider in outsourcing deals, awarding contracts and in IT procurement services.

11.1 Information security in supplier agreements

11.1.1	**Identified security requirements must be addressed, agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities.** **a) Security requirements**

Purpose: ***To ensure that risks associated with external party access to information and information systems have been mitigated by applying security controls as determined by business needs.***

11.1.1 a) Security requirements

Prior to granting access to non-public information and information systems for external parties Information Owners and Information Custodians must:

- Determine that mitigation strategies have been implemented to address security requirements;
- Review the Security Threat and Risk Assessment for asset protection requirements including:
  - Asset classification,
  - Legislative, regulatory and policy considerations, and,
  - Intellectual property rights obligations;
- Complete a Privacy Impact Assessment;
- Determine that security controls will not adversely affect target service levels; and,
- Document the roles and responsibilities of the Information Owner, Information Custodian and the external party in a formal agreement.

Recommended Tests:

Note: ISP 11.1.1 is reported on as part of the annual information security review as CO.11.4.

- Demonstrate system security requirements for external party access to government information assets are documented.
- Demonstrate there is a formal agreement for external party access to non-public information.

11.1.2	**External party access to information, information systems or information processing facilities must be based on a formal contract containing necessary information security requirements.** **a) External party access agreements** **b) Security requirements** **c) Service level continuity**

Purpose: ***To ensure external parties accessing information assets and information processing facilities are required to implement and use security controls.***

11.1.2 a) External party access agreements

Information Owners and Information Custodians must ensure access to information assets and information processing facilities by external parties is only provided after an access agreement has been completed and signed.

Access agreements must include:

- Roles and responsibilities of the Information Owner, Information Custodian and the external party;
- Non-disclosure agreements;
- Sub-contracting requirements;
- Specialized security controls (i.e., meet particular business and security arrangements, legal or regulatory requirements);
- Conditions for contract termination;
- Audit and compliance monitoring rights, responsibilities and processes;
- Reporting obligations for suspected or actual security and privacy incidents;
- Renewal and extension conditions; and,
- Requirements for regular compliance reviews.

Approved forms of agreement include:

- General Service Agreement for purchase of goods or services;
- Agreements for Alternate Service Delivery or Public Private Partnership;
- Information Sharing Agreement; or,
- Other forms of agreement as approved by Legal Services.

11.1.2 b) Security requirements

Information Owners and Information Custodians must ensure the security requirements of external party access agreements include:

- Notification of obligations of the parties to adhere to legislation and regulation;
- Requirements to adhere to agreed information security policies and procedures;
- Processes for amending the agreement;
- Acknowledgement by the external party that ownership of information is retained by the Province;
- Confidentiality obligations of the external party and their employees or agents;
- Requirements for use of unique user identifiers;
- Processes for conducting audits and compliance monitoring activities;
- Responsibilities and processes for reporting security and privacy incidents; and,
- Assurances that disciplinary action will be applied to employees or contractors who fail to comply with the terms of the agreement.

Recommended Tests:

Note: ISP 11.1.2 is reported on as part of the annual information security review as CO.11.6.

- Demonstrate third-party access agreements are in place prior to granting access.

11.1.3 Agreements with suppliers must include requirements to address the information security risks involving or associated with information and communications technology components, services and product supply chain.

a) Supplier agreement considerations

Purpose: ***To identify security controls concerning supply chain security in supplier agreements.***

11.1.3 a) Supplier agreement considerations

Information Owners and Information Custodians must identify the security risks concerning the supplier chain relationships and specify the necessary controls in the agreements.

Supply chain risk management practices should be built on top of general information security, quality, project management and system engineering practices but do not replace them. Information Owners and Information Custodians must work with suppliers to understand their supply chain and any matters that have an impact on the products and services being provided. Agreements with suppliers must address the security requirements that involve other suppliers in the supply chain. Supply chain as addressed here includes cloud computing services.

The following security controls must be considered for inclusion in supplier agreements concerning supply chain security:

- Defining information security requirements that apply to information systems and information technology product or service acquisitions;
- Requiring that suppliers apply government security requirements throughout their supply chain if the services are further subcontracted as a whole or in part;
- Requiring that suppliers apply appropriate security practices throughout the supply chain for products that include components purchased from other suppliers;
- Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;
- Implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;
- Obtaining assurance that critical components and their origin can be traced throughout the supply chain;
- Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;
- Defining the rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers; and,
- Implementing specific processes for managing information and communication technology component life-cycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Recommended Tests:

Note: ISP 11.1.3 is reported on as part of the annual information security review as CO.11.8.

- Demonstrate a review of controls in supplier agreements.
- Demonstrate supplier life-cycle management.
- Demonstrate a monitoring process for supplier agreements.
- Demonstrate contingencies for supplier disruption of services.

11.2 Supplier service delivery management

11.2.1	**Prior to using external information and technology services, security controls, service definitions and delivery levels must be identified and included in the agreement with the external party.** **a) Identifying security requirements in procurement** **b) Service level continuity**

Purpose: ***To ensure service agreements with external parties specify requirements for security and service level continuity.***

11.2.1 a) Identifying security requirements in procurement

Information Owners and Information Custodians must include security requirements in procurement documents for information and information system services being delivered by external parties. Security requirements must be documented when:

- Drafting procurement documents (e.g., Request for Information, Request for Proposal);
- Evaluating bids to confirm acknowledgement and capability;
- Preparing agreements or contracts; and,
- Developing transition and fall back plans (e.g., migration from one service provider to another).

11.2.1 b) Service level continuity

Information Owners and Information Custodians must ensure supplier service agreements document service level continuity requirements and include processes for:

- Ongoing review of service level needs with business process owners;
- Audit and compliance monitoring rights and responsibilities;
- Communicating requirements to service providers;
- Obtaining periodic confirmation from service providers that adequate capacity is maintained;
- Reviewing the adequacy of the service provider's contingency plans for responding to disasters or major service failures; and,
- Establishing the metrics for service delivery levels (including risk profiles and audit trigger levels).

Standards:

General Service Agreement and Schedule G

Recommended Tests:

Note: ISP 11.2.3 is not reported on as part of the annual information security review.

- Demonstrate the procurement document includes the Security Schedule G.
- Demonstrate the procurement document addresses the service level continuity requirements.

11.2.2	**Services provided by external parties must be regularly monitored and the reports and records reviewed.** **a) Monitoring and review of external party services**

Purpose: ***To ensure that services delivered by external parties maintain compliance with security and audit requirements.***

11.2.2 a) Monitoring and review of external party services

Information Owners and Information Custodians must establish processes to manage and review the information security of external party delivered services by:

- Assigning responsibility for monitoring to a designated employee;
- Maintaining an inventory of agreements and associated access rights;
- Monitoring for compliance through processes such as:
    - Conducting internal self-assessments of control processes,
    - Requiring external parties conduct and submit self-assessments,
    - Using embedded audit tools,
    - Requiring external parties to submit annual management assertions that controls are being adhered to,
    - Conducting independent security reviews, audits and updates to risk and controls reviews, and,
    - Analysis of audit logs;
- Establishing a process, jointly with the service provider, to monitor, evaluate, investigate and remediate incidents; and,
- Establishing performance measures within ministry service plans to ensure adequate service levels are maintained and measured.

Recommended Tests:

Note: ISP 11.2.2 is reported on as part of the annual information security review as CO.11.12.

- Demonstrate reviews are conducted on third-party delivered services.
- Demonstrate there is a process to manage and review the information security of external party delivered services.
- Demonstrate service agreements identify frequency of audits.
- Demonstrate performance measures are established and that suppliers provide adequate service levels.
- Demonstrate management signs off on the completion of audit reviews.
- Demonstrate performance measures are established to ensure adequate service levels are maintained and measured.

11.2.3 Changes to the provision of services by suppliers for information system services must take into account the criticality of the information systems, processes involved and re-assessment of risks.
a) Change management

Purpose: ***To ensure that changes to information system services delivered by external parties maintain or enhance security controls.***

11.2.3 a) Change management

Information Owners and Information Custodians must ensure agreements with external party service providers include provisions for:

- Amending agreements when required by changes to legislation, regulations, business requirements, policy or service delivery; and,
- Requiring the service provider to obtain pre-approval for significant changes involving:
    - Network services,
    - New technologies,
    - Use of new or enhanced system components (e.g., software or hardware),

- System development, test tools and facilities,
- Modification or relocation of the physical facilities, and,
- Sub-contracted services.

Information Owners and Information Custodians must ensure the change management process for information systems services delivered by external parties includes, as required:

- Reviewing and updating the Security Threat and Risk Assessment to determine impacts on security controls;
- Implementing new or enhanced security controls where identified by the risk assessment;
- Reviewing and updating the Privacy Impact Assessment;
- Initiating and implementing revisions to policies and procedures; and,
- Revising employee awareness and training resources.

Recommended Tests:

Note: ISP 11.2.3 is reported on as part of the annual information security review as CO.11.14.

- Demonstrate the change management process for information systems services delivered by suppliers is included in the service agreements.
- Demonstrate organizational agreement allows for the organization to propose and implement changes to service agreements.
- Demonstrate all changes to services provided by the supplier were authorized prior to implementation.

11.2.4 Assessment of risks from external party access to government information, information systems or information processing facilities must be undertaken and appropriate security controls implemented.
a) Risk assessment
b) Risk mitigation and acceptance

Purpose: ***To ensure the* risks *of external party access to information and information systems are identified, assessed, mitigated and managed.***

11.2.4 a) Risk assessment

Information Owners and Information Custodians are responsible for assessing the business requirements and associated risks related to external party access to information and information systems.

Risk assessments must be documented during the conceptual design phase of a project and updated throughout the life-cycle of the information system (e.g., prior to and following technical or business process changes to the information system).

The assessment of risks related to external party access must consider:

- If existing controls prevent external parties from accessing facilities or information that are not needed to meet the business requirements for the access;
- Impacts to the controls of the information processing facilities involved;
- The classification of the information assets;
- Policies and processes the external party has for employee hiring, training on security and privacy issues and incident reporting;

- Internal and external processes for managing and reporting security and privacy incidents;
- Processes for identifying, authorizing, authenticating and reviewing access rights of employees and systems of the external party;
- Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging information;
- Impacts to both parties resulting from assets being unavailable; and,
- Data integrity requirements including impacts of accessing or using inaccurate information.

11.2.4 b) Risk mitigation and acceptance

Prior to authorizing access by external parties to information and information systems, Information Owners and Information Custodians must confirm that:

- A risk and controls review has been completed and identified risks have been mitigated or accepted;
- The terms and conditions of access are documented (e.g., services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

Recommended Tests:

Note: ISP 11.2.4 is not reported on as part of the annual information security review.

- Demonstrate the risk assessment for external party access to government information has been documented.
- Demonstrate the risk assessment document has been updated throughout the life-cycle of the information system.

11.3 Cloud Computing

11.3.1 A comprehensive, documented policy on the use of cloud services must be produced and communicated to all individuals who require cloud services.
a) Cloud Computing Policy
b) Awareness requirements

Purpose: ***To ensure a consistent approach is followed regarding the procurement and use of cloud services.***

11.3.1 a) Cloud Computing Policy

Cloud computing relies on sharing resources rather than having local servers handle applications and storage. 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)).

The Cloud Computing Policy is a documented corporate policy for the purchase and use of cloud services, which is:

- Based on the Office of the Chief Information Officer's strategy;
- Approved by executive management;
- Distributed to all relevant individuals throughout government; and,

- Applied throughout government.

Information Owners are responsible for determining the information security classification of the data to be moved to a cloud service and the security requirements in using cloud computing services.

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., procurement and legal) for all cloud initiatives, and in the definition of standard and contractual requirements for the procurement and use of cloud services, to ensure that all controls and protection levels for cloud services have security by design.

11.3.1 b) Awareness requirements
Specific awareness activities must be performed to help ensure all employees:

- Are aware of the corporate policy on the use of cloud services; and,
- Are educated about the risks of using unapproved cloud services.

Recommended Tests:
Note: ISP 11.3.1 is not reported on as part of the annual information security review.

- Demonstrate the use of cloud services follows government policy and standards.

11.3.2 Information Owners and Custodians are responsible for determining the appropriateness of using a cloud service.
a) Information Security Classification
b) Security of cloud services
c) Technical specifications

Purpose: ***To ensure a consistent approach is followed regarding the procurement and use of cloud services.***

11.3.2 a) Information Security Classification
Information Owners must first determine the security classification of the data to be transmitted, processed and/or held in the cloud before the data can be moved to the cloud. The information security classification of the data is assessed on whether the data contains personal information, its sensitivity, confidentiality and criticality to business operations (e.g., commercial information, intellectual property (IP), legal, regulatory and privileged information (LRP), logistical information, management information).

Information Owners and Information Custodians must also complete a Privacy Impact Assessment before moving the data to the cloud as part of the process of determining the security classification of the data. The context in which the data will be gathered or used in the cloud service will be an important factor in the Privacy Impact Assessment as well.

11.3.2 b) Security of cloud services
Information Owners and Information Custodians must:

- Conduct a Security Threat and Risk Assessment to determine whether the cloud service is appropriate for the information security classification of the data to be transmitted, processed, and/or stored in the cloud based on legal and regulatory risks to government (e.g., copyright, data protection, financial regulation, privacy protection and corporate governance);

- Document, maintain and verify that all information security provisions for the use of cloud services are based on the information security classification of the data that will be transmitted, processed and/or stored in the cloud; and,
- Determine that the cloud vendor can provide the required information security measures that are determined by the information security classification of the data to be transmitted, processed and/or stored in the cloud.

11.3.2 c) Technical specifications

Use of cloud services must not weaken the security of existing systems and infrastructure. Information Owners and Information Custodians must ensure that technical means of protecting information placed in the cloud include:

- A technical security infrastructure that is compatible with the architecture and infrastructure used by the cloud service provider;
- Compatibility of client systems for each cloud service with corporate standards (e.g., by monitoring browser version and plug-in requirements);
- Use of secure communication techniques between government and cloud services (e.g., by deploying VPN, TLS, HTTPS or similar);
- Availability of electronic discovery or equivalent access to search and preserve log data in order to enable and support security investigations, evidence collection and response to legal hold requests; and
- Availability of automated technologies to log, monitor, correlate and alert across the infrastructure that is providing the cloud services to ensure that security breaches and compromises are detected and addressed adequately by the cloud service provider;

Sensitive information stored and processed in the cloud must be protected against co-mingling by separating the organisation's information from that of other organisations. The use of encryption, obfuscation or tokenization is required when using cloud services to protect the confidentiality and integrity of the information.

Guidelines:

Encryption, tokenization of the data does not always guarantee the confidentiality of the data. Depending on how the various standards are adopted by the cloud vendor, security of the data placed with the cloud vendor is not guaranteed even if the vendor attests to a long list of certifications.

Recommended Tests:

Note: ISP 11.3.2 is reported on the annual information security review as CO.11.6.

- Demonstrate that the information to be moved to the cloud has an information security classification.
- Demonstrate a Security Threat and Risk Assessment and Personal Impact Assessment have been completed for the cloud service.
- Demonstrate that the cloud vendor has been assessed against a standard or a set of standards (e.g., ISO 27001, ISO 27017, ISO 27018, NIST 800-53, Cloud Control Matrix, HIPAA, PCI, etc.)

11.3.3 The use of cloud services must not impede the availability of information and information services.
a) Assurance of information availability

Purpose: ***To ensure the continued availability of information required to conduct business.***

11.3.3 a) Assurance of information availability

Information Owners and Information Custodians must ensure the availability of access to information stored in the cloud by:

- Investing in robust, reliable Internet connectivity;
- Establishing multiple methods of connection (e.g., wired network, wireless and 3G/4G);
- Providing required network bandwidth between the organisation's network and the cloud service provider to avoid poor network latency; and,
- Maintaining links with the legacy systems.

Guidelines:

Poor network connectivity can affect end user experience, availability of cloud services, and if severe enough, can cause data corruption as well. End user experience must be taken into account when designing the infrastructure to connect to the cloud as it impacts cloud adoption.

Recommended Tests:

Note: ISP 11.3.3 is not reported on the annual information security review.

12 Information Security Incident Management

This chapter establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that employees understand their roles in reporting and mitigating security events.

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts to continually improve and strengthen the information security infrastructure of the Province.

12.1 Management of information security incidents and improvements

12.1.1 Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.
a) Information security incident management

Purpose: ***To enable quick and orderly management of information security incidents.***

12.1.1 a) Information security incident management

Information Owners and Information Custodians must adopt the Information Security Incident Management Process and ensure that those responsible for information security incident management understand the priorities for handling information security incidents.

Ministries must follow the established Information Incident Management Process for reporting, managing, responding to and recovering from information security incidents. The process must include:

- Procedures for incident response planning and preparation;
- Procedures for monitoring, detecting, analyzing and reporting of information security incidents;
- Procedures for logging incident management activities; and,
- Procedures for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans.

Employees with security incident management responsibilities must be appropriately trained and deemed qualified (e.g., in forensics and investigations), and their authorization for access to live systems and data must be delineated formally. Incident response processes must be documented, tested and rehearsed regularly to evaluate their effectiveness.

In case of an information security incident, the Investigations and Forensics Unit of the Office of the Chief Information Officer must be provided access to all and any relevant primary data stores in a quick, effective and expedient manner to ensure an orderly response to incidents.

The Information Incident Management Process includes the following documents:

- Information Incident Management Process document;
- Information Incident Report Form;
- Easy Guide for Responding to Information Incidents;
- Process for Responding to Privacy Breaches; and,
- Information Incident Checklist.

Guidelines:
Potential types of security incidents to be reported include:

- Suspected or actual breaches of privacy and/or confidentiality;
- Denial of service;
- Detection of network probing;
- Detection of malicious code (e.g., virus, worm, Trojan horse);
- Errors due to incomplete or inaccurate data;
- Outgoing network traffic not associated with typical business processing;
- Repeated attempts of unauthorized access;
- Inappropriate use of government information resources;
- Repeated attempts to e-mail unknown internal accounts;
- System activity not related to typical business processing;
- System failures and loss of service;
- Privacy breaches of personal information;
- Responses to phishing attacks;
- Threatening or harassing communication; and,
- Sharing of user credentials.

Employees who regularly ignore information security and privacy policies should be subject to a disciplinary process that includes notification of their Supervisor and suspension of privileges for repeated offences.

Recommended Tests:
Note: ISP 12.1.1 is reported on as part of the annual information security review as CO.12.4.

- Demonstrate that employees are made aware of the Information Security Incident Management Process.
- Demonstrate that employees follow the Information Security Incident Management Process for reporting and responding to information security incidents.

12.1.2 Information security events must be reported immediately.
a) Reporting information security events
b) Information security event logging

Purpose: ***To enable prompt response to information security events and identify government wide trends.***

12.1.2 a) Reporting information security events
As required by the Information Incident Management Process, employees must immediately report all suspected or actual information security events as quickly as possible to their Supervisor. Your Supervisor will ensure that senior managers and your Ministry Chief Information Officer are also informed. You or your Supervisor must also immediately notify the Office of the Government Chief Information Officer by dialling the OCIO Helpdesk at 250 387-7000 or toll-free at 1-866 660-0811 and selecting Option 3 and asking for an Information Incident Investigation. You will be contacted shortly by the Government Chief Information Officer's Investigations Unit, which will seek further details and may give advice on next steps.

All employees must be aware of:

- Procedures for reporting information security events; and,
- Points of contact for reporting.

Requirements for reporting events must be included in contracts and service agreements.

Situations to be considered for information security event reporting include:

- Ineffective security controls;
- Breach of information integrity, confidentiality or availability expectations;
- Breach of personal privacy;
- Human errors;
- Non-compliance with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware; and,
- Access violations.

12.1.2 b) Information security event logging

Information security event logs are logs that could be used in security investigations, auditing or monitoring and could give rise to a security incident. Security events may be any activities that can potentially impact the confidentiality, integrity or availability of government information in both paper and electronic format.

Information security event logs are notification or alert that a device or software may be technically capable of producing, and are related to its status (e.g., configurations changes, log-on or log-off events), or its function and activities (e.g., data, traffic or sessions routed, transmitted, blocked, permitted). Information security event logging must always be enabled to provide context and data to support security investigation, audit, and monitoring.

Information security event logging is not limited to security devices, but is applicable to any and all devices, systems, software or applications that can produce logs that can be used to validate the confidentiality, integrity or availability of government information whether in security investigations, auditing or ongoing monitoring. Examples of devices, systems, software or applications that can produce information security logs include, but are not limited to, routers, switches, content filtering, network traffic flow, network firewalls, Intrusion Prevention/Detection Systems, servers, applications, databases, operating systems, application firewalls, authentication services, directory services, DHCP, DNS, and hardware platforms.

All devices, systems, software or applications that have logging capabilities must be configured to produce logs to enable the detection of security events and intrusions that otherwise would go undetected without such logging.

If the logging that the device or software is technically capable of producing is disabled or only partially configured, then this decision must be documented and include the rationale for deactivating or only partially implementing the logging. The corresponding Security Threat and Risk Assessment must be updated to reflect this decision and must assess whether the risk introduced by the lack of logging is acceptable.

Guidelines:
The Information Incident Management Process should be part of the Ministry Business Continuity Program. The awareness program should build trust with employees and stress that "to err is human". Positive reinforcement of good computing and reporting practices will help employees understand their responsibilities. Employees who commit errors that lead to security incidents should receive appropriate training and counselling.

Recommended Tests:
Note: ISP 12.1.2 is reported on as part of the annual information security review as CO.12.6.

- Demonstrate employees are made aware of the Information Incident Management Process.

12.1.3 Employees using the organization's information systems must note and report any observed or suspected security weaknesses in those systems.
a) Reporting security weaknesses

Purpose: To assist in maintaining the security of information systems.

12.1.3 a) Reporting information security weaknesses
All employees must report as quickly as possible any observed or suspected security weaknesses in information systems. Ministries must follow the Information Incident Management Process for responding to suspected or actual security weaknesses which includes:

- Reporting to the Ministry Chief Information Officer, Risk Management Branch and Government Security Office, and the Office of the Government Chief Information Officer as appropriate. The response process must:
  - ensure all reports are investigated and handled in a secure, confidential manner, and,
  - ensure the individual who reported the weakness is advised of the outcome when the investigation is complete; and,
- A user awareness program on information security advising employees that:
  - they have a responsibility to report observed or suspected weaknesses to the Ministry point-of-contact,
  - suspected or observed weaknesses must not be tried or tested, and,
  - weaknesses should not be discussed, or made known, except through approved reporting channels.

Guidelines:
The reporting and response processes for all security weaknesses, threats, events and incidents should be consolidated to avoid duplication and establish a consistent approach.

Recommended Tests:
Note: ISP 12.1.3 is reported on as part of the annual information security review as CO.12.8.

- Demonstrate employees are made aware of the Information Incident Management Process as a mechanism for reporting security weaknesses.

12.1.4 Information security events must be assessed to determine if an information security incident has occurred.

a) Assessment of and decision on information security events

Purpose: ***To help assess and classify events to identify if they are information security incidents.***

12.1.4 a) Assessment of and decision on information security events

The Chief Information Security Officer must assess each information security event using the agreed upon information security event and incident classification scale and decide whether the event should be classified as an information security incident. An information incident is 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.

Results of assessments and decisions should be recorded in detail and provided to the Office of the Government Chief Information Officer.

Recommended Tests:

Note: ISP 12.1.4 is reported on as part of the annual information security review as CO.12.10.

- Demonstrate documentation identifying an information security event investigation escalation process.
- Demonstrate a formal review of an incident complete with recommendations.

12.1.5 Information security incidents must be responded to in accordance with the documented procedures.

a) Response to information security incidents

Purpose: ***To identify in advance of an information security incident, the authority to respond in a controlled manner.***

12.1.5 a) Response to information security incidents

Information security incidents must be responded to by the Chief Information Security Officer and other relevant employees of the organization or external parties.

The response should include the following:

- Collecting evidence as soon as possible after the occurrence;
- Conducting information security forensics analysis, as required;
- Escalation, as required;
- Ensuring that all involved response activities are properly logged for later analysis;
- Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;
- Dealing with information security weaknesses found to cause or contribute to the incident; and,
- Once the incident has been successfully dealt with, formally closing and recording it.

The goals of incident response are to resume 'normal security level' and to initiate the necessary recovery. Post-incident analysis should take place, as necessary, to identify the source of the incident.

Recommended Tests:

Note: ISP 12.1.5 is reported on as part of the annual information security review as CO.12.12.

- Demonstrate post incident analysis includes recommended corrective measures.

12.1.6 Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.
a) Learning from information security incidents

Purpose: ***To identify and use information security incident trends to update the Information Security Policy and supporting security processes.***

12.1.6 a) Learning from information security incidents

The Chief Information Security Officer is responsible for monitoring and evaluating information security incidents by:

- Using statistical analysis of incident frequency, type and location to identify trends;
- Ensuring incident reports and trends are used to promote continuous improvement of security policies and processes, security awareness and training programs, and business continuity and disaster recovery plans;
- Advising Information Owners and Information Custodians and Ministry Information Security Officers of evolving security exposures and mitigation strategies;
- Evaluating the effectiveness of incident management, response and reporting; and,
- Evaluating the effectiveness of information security technologies.

The Chief Information Security Officer must provide incident information to the Office of the Government Chief Information Officer, Risk Management Branch and Government Security Office, and the Office of the Comptroller General as appropriate.

The Information Security Branch, Office of the Government Chief Information Officer, is the centre of expertise and an essential capability in security incident protection, detection, response and correction where employees assigned responsibility for information incident management receive special training in managing crises across the spectrum of potential incidents.

The Information Security Branch must provide incident analysis to the Office of the Government Chief Information Officer and Risk Management Branch and Government Security Office as the focus of security incident reporting, management and improvement within government. Information sharing with stakeholder and partner organizations, other provincial security incident response centres and national incident response centres should also be fostered. Information security incident response must be integrated within the broader requirements for business continuity and disaster recovery. Integration will simplify processes, maintain consistency and eliminate duplication.

Continuous improvement of security incident management processes includes:

- Monitoring incidents using statistical analysis of frequency, types and locations of security incidents;
- Analysis of incidents, responses and successful containment;
- Determining requirements for user awareness and training;
- Improving the security of information systems through monitoring and reporting; and,
- Integrating automated alarms and other security incident detection technology with user reporting, checking logs and auditing systems.

Recommended Tests:

Note: ISP 12.1.6 is reported on as part of the annual information security review as CO.12.14.

- Demonstrate Information Owners, Information Custodians and Ministry Information Security Officers are made aware of security issues and an action plan is formulated to mitigate further risks of exposure.
- Demonstrate that information incident trends are analyzed to inform decision-making.

12.1.7 Investigations into information security incidents must ensure evidence is identified, collected, preserved, retained and presented in conformance with the rules for collection of evidence.
a) Information security incident investigation
b) Collection of evidence

Purpose: ***To ensure investigation processes preserve the integrity of evidence that may be required for legal or disciplinary action.***

12.1.7 a) Information security incident investigation

Information security incident investigation must be formalized and practiced in accordance with standard investigation techniques:

- Information security incident investigation processes include:
  - identification of the incident cause,
  - planning of corrective action,
  - implementation of corrective action to prevent recurrence, and,
  - reporting action taken;
- Employees with responsibilities for information security investigations (investigating officers) must be aware of processes for securing potential evidence such as technology assets, audit logs, audit trails, voice mail and e-mail accounts for analysis and as potential evidence in legal proceedings;
- Inappropriate use of information and technology resources requires that within 48 hours the investigating officer contact:
  - in the case of an employee the individual's excluded Supervisor and BC Public Service Agency (BCPSA) Labour Relations; and,
  - in the case of a contractor or business partner the contract manager or relationship manager;
- When criminal activity is suspected, the investigating officer must ensure that the appropriate law enforcement authorities are contacted. Before contacting law enforcement authorities, the Risk Management Branch and Government Security Office and the Office of the Government Chief Information Officer must be consulted;
- On resolution of an information security incident or weakness, the investigating officer must prepare a report that includes a detailed problem analysis, actions taken, and recommendations for corrective action or improvements; and,
- Information security incident reports must be submitted to Information Owners, Information Custodians, senior management, Office of the Government Chief Information Officer and Risk Management Branch and Government Security Office as part of security program management.

In order to enable quick, effective and immediate response to information security incidents and breaches, employees with responsibilities for security investigations (investigating officers) must be able to access security log data and security log data processing and reporting facilities immediately. This

access will be for the purposes of evidence collection as well as security log parsing, searching, and reporting to enable identification, root cause analysis, and resolution of breaches and incidents. Access will be configured and enabled for on-line, real-time access to the GUI (Graphical User Interfaces)/Consoles/Interfaces of:

- The systems that generate and produce security log data and feature an interface that has reporting, parsing or searching functions with relation to the security log data it generates;
- The centralized log management system, service or facilities; and,
- The centralized monitoring system, service or facilities.

If the specific technology does not have a GUI/Console/Interface available, and instead relies on raw log data generation, equivalent functionality that permits the timely and effective searching of the security logs produced must be implemented.

12.1.7 b) Collection of evidence

At the outset of an information security investigation it may not be known if legal or disciplinary actions will result and what evidence will be required. To ensure proper procedures, confidentiality and information privacy, evidence must only be collected by individuals authorized by the Chief Information Security Officer.

- Evidence collection procedures must be documented by the Chief Information Security Officer;
- Investigative processes must follow the rules of evidence to ensure relevance, admissibility and materiality; and,
- Information Owners and Information Custodians in receipt of a legal order to produce electronic evidence must immediately contact the Chief Information Security Officer.

Guidelines:

In general, procedures for evidence collection should include identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and the status of devices (e.g., powered on or off). The procedures should take account of:

- Chain of custody;
- Safety of evidence;
- Safety of employees;
- Roles and responsibilities of employees involved;
- Competency of employees;
- Documentation; and,
- Briefing.

Recommended Tests:

Note: ISP 12.1.7 is reported on as part of the annual information security review as CO.12.16.

- Demonstrate that in instances that collection of evidence was required, that it was done under the direction of the Chief Information Security Officer.

13 Information Security Aspects of Business Continuity Management

This chapter provides direction from a security focus for planning the resumption of business or services where a man-made or natural disaster has occurred. Government organizations are required to be prepared and to re-establish business or services as swiftly and smoothly as possible. Business continuity plans include the evaluation of security risks in line with the directions set by Emergency Management BC and the BC government. More comprehensive policy on business continuity management is described in Chapter 16 of the government Core Policy and Procedures Manual.

13.1 Information security continuity

13.1.1 The organization must determine its requirements for information security and the continuity of information security management in adverse situations.

a) Business continuity planning

b) Business continuity risk assessment

c) Business continuity strategy

d) Business continuity plans

e) Coordination of business continuity plans

Purpose: ***To ensure government can continue to deliver essential services despite damage, loss, or disruption of business processes.***

13.1.1 a) Business continuity planning

Information Owners and Information Custodians must ensure business continuity and recovery plans address information security requirements consistent with the classification of the information. Processes for establishing business continuity and recovery plans are detailed in the Business Continuity Management Program Guidelines.

- Information Owners must perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations; and,
- Information security requirements remain the same in adverse situations, compared to normal operational conditions.

The Information Custodian must maintain the business continuity and recovery plans for information systems as part of the System Security Plan.

Government policy on business continuity programs is defined in Core Policy and Procedures Manual 16 – Business Continuity Management.

13.1.1 b) Business continuity risk assessment

The process for identifying, analyzing and evaluating risks, including information security risks, is detailed in the Business Continuity Management Program Guidelines, section 2 – Identify, Analyze and Evaluate Risks.

The process for analyzing and assessing business impacts, including those for information security risks, is detailed in the Business Continuity Management Program Guidelines, section 3 – Review Business Functions and Analyze Business Impacts.

13.1.1 c) Business continuity strategy
The process for developing a business continuity strategy is detailed in the Business Continuity Management Program Guidelines, section 4 – Plan Mitigation Strategies and, section 5 – Plan Business Continuity Strategies.

13.1.1 d) Business continuity plans
Requirements for business continuity plans are defined in Core Policy and Procedures Manual 16 – Business Continuity Management. The process for developing and maintaining business continuity plans is detailed in the Business Continuity Management Program Guidelines.

13.1.1 e) Co-ordination of business continuity plans
Information Owners and Information Custodians must ensure business continuity plans:

- Include the classification of information assets to identify critical business operations;
- Use government-wide frameworks and processes; and,
- Use information security processes which maintain approved security levels.

The Emergency Management BC must coordinate government-wide business continuity plans to reconcile recovery priorities, business impacts, security impacts and business resumption processes.

The Government Chief Information Officer is responsible for protecting the privacy, confidentiality, integrity and availability of government's electronic information. This responsibility includes providing expert advice to Emergency Management BC on information security aspects of business continuity plans.

Recommended Tests:
Note: ISP 13.1.1 is reported on as part of the annual information security review as CO.13.4.

- Demonstrate a documented business continuity plan that is current, reviewed regularly and is aligned with government strategic objectives.

13.1.2 The organization must establish, document, implement and maintain processes, procedures and controls to ensure the required level of information security for business continuity during an adverse situation.
a) Implement required level of continuity
b) Information security continuity requirements
c) Processes and procedures
d) System redundancy

Purpose: ***To ensure the required level of continuity for information security is maintained during an adverse situation.***

13.1.2 a) Implement required level of continuity
Information Owners and Information Custodians must ensure that:

- An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using employees with the necessary authority, experience and competence;
- Incident response employees with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated; and,
- Documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on approved information security continuity objectives.

13.1.2 b) Information security continuity requirements

According to the information security continuity requirements, Information Owners and Information Custodians must establish, document, implement and maintain:

- Information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- Processes, procedures and implementation changes to maintain existing information security controls during an adverse situation; and,
- Compensating controls for information security controls that cannot be maintained during an adverse situation.

13.1.2 c) Processes and procedures

Within the context of business continuity or disaster recovery, specific processes and procedures have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them must be protected. Information Owners and Information Custodians must involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

13.1.2 d) System redundancy

Information security controls that have been implemented must continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls must be established, implemented and maintained to achieve an acceptable level of information security.

Recommended Tests:

Note: ISP 13.1.2 is reported on as part of the annual information security review as CO.13.6.

- Demonstrate a management structure is in place to mitigate and respond to adverse situations.
- Demonstrate documented plans, response and recovery procedures are developed and approved.
- Demonstrate compensating controls for information security controls that cannot be maintained during an adverse situation have been developed.

13.1.3 Business continuity plans must be regularly exercised and updated.
a) Business continuity plan exercising and maintenance

Purpose: ***To ensure business continuity plans are current, functional and address information security requirements.***

13.1.3 a) Business continuity plan exercising and maintenance

Information Owners and Information Custodians must review business continuity plans annually to ensure they are current, valid and readily accessible during a business interruption. Business Continuity Plans must be coordinated with security management and emergency preparedness and response plans.

Business Continuity Plans must be exercised at least annually to the extent necessary to confirm plan effectiveness and to ensure employees are prepared and trained. All employees and key stakeholders must be aware of the Ministry Business Continuity Management Program and understand its contents and their role. Information Owners and Information Custodians must report the number and type of exercises completed, the training conducted and the status of the business continuity plans to Emergency Management BC semi-annually.

Requirements for exercising business continuity plans are defined in Core Policy and Procedures Manual 16 – Business Continuity Management. The processes for exercising business continuity plans are detailed in the Business Continuity Management Program Guidelines, section 8 – Train and Exercise. Requirements for the maintenance of the business continuity plan are detailed in Business Continuity Management Program Guidelines, Section 10 – Monitor and Review.

Recommended Tests:
Note: ISP 13.1.3 is reported on as part of the annual information security review as CO.13.8.

- Demonstrate the business continuity plan is reviewed and tested annually.
- Demonstrate employees are made aware of their roles and responsibilities as part of the business continuity plan.

13.2 Redundancies

13.2.1 Information processing facilities must be implemented with redundancy sufficient to meet availability requirements.
a) Availability requirements

Purpose: To ensure the availability of information systems without interruption.

13.2.1 a) Availability of information processing facilities
The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems. Information Owners and Information Custodians must identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.

Where applicable, redundant information systems must be tested to ensure the failover from one component to another component works as intended.

Recommended Tests:
Note: ISP 13.2.1 is reported on as part of the annual information security review as CO.13.12.

- Demonstrate system redundancy capacity is adequate to meet system service business requirement.

14 Compliance

This chapter describes requirements for verifying that information systems comply with relevant statutory, regulatory, and information security contractual clauses. Compliance policies identify what to do to ensure that the Province is in compliance with applicable laws and policies. Processes to monitor the extent to which information systems follow policies include conducting security reviews, assessments and the systematic analysis of logged information.

14.1 Compliance with legal and contractual requirements

14.1.1 The legislative, statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.
a) Applicable legislation and contractual requirements

Purpose: ***To ensure that the legal requirements of information systems are documented.***

14.1.1 a) Applicable legislation and contractual requirements

Information Owners are responsible for ensuring that legislative statutory, regulatory, policy and contractual requirements of each information system are:

- Identified and documented when commencing a system development or enhancement initiative;
- Reviewed prior to, or concurrent with, changes to legislation, regulation or policy; and,
- Explicitly identified in contracts and service agreements, and included in:
  - Privacy Impact Assessments,
  - Security Threat and Risk Assessments,
  - System Security Plans,
  - Risk Management Plans, and,
  - Business Continuity Plans.

Privacy requirements for information systems containing or handling personal information are defined in the Freedom of Information and Protection of Privacy Act - Policy and Procedures Manual and the Core Policy and Procedures Manual (CPPM).

Recommended Tests:

Note: ISP 13.2.1 is reported on as part of the annual information security review as CO.13.12.

- Demonstrate that legislative, statutory, regulatory, policy and contractual requirements of each information system are identified and documented.

14.1.2 Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licencing.
a) Intellectual property rights of external creators and owners
b) Intellectual property rights for government assets

Purpose: ***To protect the intellectual property rights of information and software creators and owners.***

14.1.2 a) Intellectual property rights of external creators and owners
Information Owners and Information Custodians must protect intellectual property by:

- Ensuring that information and software is only acquired from reputable vendors;
- Maintaining proof or evidence of ownership or right to use;
- Adhering to the terms and conditions of use associated with intellectual property;
- Ensuring the maximum number of users permitted is not exceeded;
- Implementing processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licences;
- Requiring the removal of unlicensed information and software from government information systems;
- Informing employees of government policies, including the Appropriate Use Policy;
- Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
- Complying with terms and conditions for information and software obtained from public networks (e.g., "free for personal use only", open source).

14.1.2 b) Intellectual property rights for government assets
Policy for the intellectual property of government information assets is in the Core Policy and Procedures Manual 6.3.4 – Corporate Supply and Disposal Arrangements which is managed by the Intellectual Property Program of the Office of the Government Chief Information Officer.

Recommended Tests:
Note: ISP 11.1.2 is reported on as part of the annual information security review as CO.14.6.

- Demonstrate software is only acquired through reputable sources, and that copyright is not violated.
- Demonstrate asset registers, maintaining evidence of ownership of licences, maximum number of users permitted within the licence and carrying out review.
- Demonstrate licencing agreements for software provide evidence of adherence to terms and conditions.
- Demonstrate Ministry-developed intellectual property has the appropriate copyright notices.
- Demonstrate investigations or reviews are conducted to detect unlicensed software.

14.1.3 Government records must be protected from loss, destruction and falsification, unauthorized access, release, and disposal in accordance with legislative, regulatory, contractual and business requirements.
a) Protection of records

Purpose: To ensure compliance with legislative and policy requirements for government records.

14.1.3 a) Protection of records
When deciding upon protection of specific organizational records, Information Owners and Information Custodians must consider the information security classification.

Information Owners and Information Custodians must ensure the protection of records by:

- Using government guidelines on the retention, storage, handling and disposal of records and information;

- Following a retention schedule identifying records and the period of time for which they should be retained; and,
- Maintaining an inventory of sources of key information.

Disposal of government records must follow the records schedule as defines in the Information Management Act. Policy requirements for records management are in the Core Policy and Procedures Manual 12.3.3 – Information Management, and the Recorded Information Management Manual.

Recommended Tests:
Note: ISP 14.1.3 is reported on as part of the annual information security review as CO.14.8.

- Demonstrate that employees are made aware of and follow the document disposal requirements.

14.1.4 Privacy and protection of personal information must be ensured as required in legislation and regulation.
a) Privacy and protection of personal information

Purpose: ***To ensure the privacy and protection of personal information in compliance with legislation.***

14.1.4 a) Privacy and protection of personal information
Information Owners and Information Custodians must document and implement policies for privacy and the protection of personal information. The policy must be communicated to all employees involved in the processing of personal information. There must be Privacy Impact Assessment and Security Threat and Risk Assessment documents for all operations areas that are collecting, processing and storing personal information.

The Freedom of Information and Protection of Privacy Act requires personal information to be protected using 'reasonable security measures'.

The Information Security Policy includes detailed controls which enable and support the protection of government information and information systems.

Recommended Tests:
Note: ISP 14.1.4 is reported on as part of the annual information security review as CO.14.10.

- Demonstrate user awareness is provided for dealing with personal information.

14.1.5 Controls must be in place to deter misuse of information systems.
a) Deterring unauthorized and inappropriate use of information systems

Purpose: ***To ensure employees do not create security exposures through unauthorized or inappropriate use of information systems.***

14.1.5 a) Deterring unauthorized and inappropriate use of information systems
Information Owners and Information Custodians must monitor information system usage to prevent, detect and respond to unauthorized or inappropriate use by:

- Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage;

- Implementing processes to analyze audit logs to identify potential misuse of information systems;
- Implementing system rules to prevent access to undesirable Internet sites;
- Implementing content inspection and filtering tools (e.g., for e-mail and web traffic);
- Immediately notifying employees of detected misuse (e.g., the 'Red Screen' for Internet blocking);
- Ensuring that security incidents are investigated in accordance with policy; and,
- Determining, in consultation with the BC Public Service Agency, if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for employees who have made unauthorized or inappropriate use of information system resources.

Prior to implementing information system monitoring processes, Information Owners and Information Custodians must ensure:

- Monitoring activities are compliant with legislative, legal, policy and contractual requirements and obligations;
- Employees are informed that specific activities may be monitored; and,
- Access to data gathered through monitoring processes is restricted on a 'need-to-know' and 'least privilege' basis to the fewest possible number of users.

Recommended Tests:

Note: ISP 14.1.5 is not reported on as part of the annual information security review.

- Demonstrate audit logs are reviewed on a regular basis.

14.1.6 Cryptographic controls must be used in compliance with relevant agreements, legislation and regulations.
a) Regulation of cryptographic controls

Purpose: ***To prevent inappropriate use and unregulated importing or exporting of cryptographic controls.***

14.1.6 a) Regulation of cryptographic controls

When cryptographic controls are used, Information Owners and Information Custodians must:

- Ensure that the use of cryptographic control(s) is supported by an Information Security Threat and Risk Assessment;
- Consult with the Corporate Information and Records Management Office and Office of the Government Chief Information Officer regarding the records management, electronic commerce, information access, privacy and security issues prior to acquiring cryptographic controls;
- Ensure encrypted government information assets do not become unavailable due to unavailability or loss of cryptographic keys by implementing a process to manage cryptographic keys as defined by the Government Chief Information Officer; and,
- When acquiring cryptographic controls from outside Canada, the procurement must be from a reputable vendor who can provide reasonable assurance on the legality of import into Canada.

The Office of the Government Chief Information Officer will:

- Develop and document cryptographic key management processes;

- Provide guidance and assistance to Ministries and agencies in the selection and use of cryptographic controls; and,
- Establish and publish cryptographic standards.

Recommended Tests:
Note: ISP 13.2.1 is reported on as part of the annual information security review as CO.13.12.

- Demonstrate cryptographic controls are used as required.

14.2 Information security reviews

14.2.1 Independent reviews of information security must be regularly conducted.
a) Independent review of information security
b) Remediation

Purpose: ***To provide an assessment of the Information Security Program.***

14.2.1 a) Independent review of information security
Independent reviews are necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security. The review must include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

The Chief Information Security Officer must initiate an independent third party review of the Information Security Program every two years including:

- Assessing the operational effectiveness of the Information Security Program;
- Documenting the results; and,
- Reporting the results of the review to senior management.

14.2.1 b) Remediation
Information Owners and Information Custodians must address the identified weaknesses and non-compliant controls prior to the next review.

Recommended Tests:
Note: ISP 14.2.1 is reported on as part of the annual information security review as CO.14.16.

- Demonstrate a review of the information security program has been conducted by an independent third party.

14.2.2 Information Owners must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.
a) Compliance with security policies and standards
b) Review of controls
c) Review of implementation of information incident report recommendations

Purpose: ***To ensure compliance of information systems with information security policy, requirements and standards.***

14.2.2 a) Compliance with security policies and standards
Information Owners must ensure security policies and processes are implemented and adhered to by:

- Conducting periodic self-assessments;
- Ensuring employees receive regular information security awareness updates; and,
- Initiating independent assessments, reviews or audits to assess compliance with policy.

When review processes indicate non-compliance with policies, Information Owners must:

- Determine cause(s);
- Assess the threats and risks of non-compliant processes;
- Document the marginal risks where required; and,
- Develop plans to implement corrective action.

14.2.2 b) Review of controls
Information Owners must develop an annual plan which identifies information systems scheduled for a security review in each fiscal year. The information systems to be reviewed in each year should be:

- Determined in conjunction with the Ministry Enterprise-wide Risk Management Plan;
- Endorsed by the Ministry Audit Committee, or equivalent; and,
- Reported as part of the annual information resource management plan.

Information Owners must ensure that critical information systems are reviewed at least every three years.

14.2.2 c) Review of implementation of information incident report recommendations
Information Owners and Information Custodians must ensure that recommendations from information incident reports are addressed.

The Chief Information Security Officer may perform compliance reviews or audits of the implementation of recommendations from information incident reports, when necessary. The Ministry Chief Information Officer must ensure that Information Owners and Information Custodians support the audit activities.

Guidelines:
When determining the review frequency for information systems consider:

- The value of the information system as determined by a Security Threat and Risk Assessment or a Risk and Controls Review;
- Frequency of changes or updates (as changes may introduce new risks, a system which has undergone frequent changes may have higher risks); and,
- Results of previous reviews.

Internal Audit and Advisory Services, Office of the Comptroller General, should be consulted prior to issuing Requests for Proposals or contracts for independent information security reviews or audits. Self-assessment tools are available from Information Security Branch, Office of the Government Chief Information Officer.

Recommended Tests:
Note: ISP 14.2.2 is reported on as part of the annual information security review as CO.14.18.

- Demonstrate issues identified in the annual Ministry information security compliance review are reviewed and addressed.

14.2.3	**Information systems must be regularly reviewed for compliance with security policies and standards.** **a) Technical compliance checking** **b) Authorization to conduct technical compliance checking** **c) Reporting results**

Purpose: ***To determine if technical controls meet established government standards.***

14.2.3 a) Technical compliance checking

Information Custodians must regularly test information system technical control compliance by using automated tools to:

- Detect network intrusion;
- Conduct penetration testing;
- Determine if information system patches have been applied;
- Confirm that system technical controls have been implemented and are functioning as designed; and,
- Perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or systems changes have not been made.

14.2.3 b) Authorization to conduct technical compliance checking

Supervisors responsible for technical compliance checking and Information Custodians must ensure that:

- Information Owners and operations employees are consulted prior to initiating tests;
- The Chief Information Security Officer is notified prior to testing to prevent triggering false security alarms from the infrastructure; and,
- Automated testing of operational systems is conducted by employees authorized by the Chief Information Security Officer.

Ministries must consult with the Chief Information Security Officer prior to issuing Requests for Proposal or contracts for technical compliance checking.

14.2.3 c) Reporting results

Supervisors responsible for technical compliance checking and Information Custodians must:

- Assess results of testing and promptly develop action plans to investigate and mitigate identified exposures in consultation with the Ministry Information Security Officer;
- Provide Information Owners and the Chief Information Security Officer with copies of test results and action plans;
- Provide the Chief Information Security Officer with the internal or external audit reports immediately upon receipt; and,
- Maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

Guidelines:

The Chief Information Security Officer should:

- Develop and maintain testing processes for authorizing/conducting tests, storing results and building on previous testing experience; and,
- Provide summarized quarterly reports to the Government Chief Information Officer on the status and results of testing.

Recommended Tests:

Note: ISP 14.2.3 is reported on as part of the annual information security review as CO.14.20.

- Demonstrates vulnerability testing on a regular basis, that controls are functioning, that patches are applied.
- Demonstrate authorization from the Information Owner is obtained prior to technical compliance testing.
- Demonstrate an action plan that documents control weaknesses and the verification of remediation.
- Demonstrate the Chief Information Security Officer is notified prior to technical testing.
- Demonstrate that Information Owners and Information Custodians provide copies of reviews and audit reports to the Chief Information Security Officer.

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 Policy, 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 in 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 – is 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, 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 policy 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 Program – See: Information Security Policy 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, assessments done in iSMART tool, vulnerability testing, penetration testing, audit reviews. The government standard for STRAs, however is the iSMART.
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***.