6.19 INFORMATION SECURITY STANDARD SPECIFICATION

Abstract

Supporting document for the IMIT 6.19 Information Security Standard. It provides clarification and additional requirements of the standard.

Information Security Branch

infosecadvisoryservices@gov.bc.ca

Contents

1. INTRODUCTION

This specification document was developed to provide detailed security requirements to support the **IMIT 6.19 Information Security Standard** (ISS) (version 3.0). The specifications outlined in this document must be followed in conjunction with the standard.

The purpose of this document is to assign responsibilities for the deliverables of this standard, define terms and definitions and provide a linkage to **Defensible Security Framework** and detailed requirements of the security roles and security responsibilities.

As the other IMIT standards referred to in Sections 5.3 through 5.15 of the IMIT 6.19 ISS have their own corresponding specification documents, this document will not address those standards.

2. DEFENSIBLE SECURITY LINKAGE

The IMIT 6.19 ISS establishes the baseline security controls required to establish adequate information security in accordance with government's **Defensible Security Framework** for the protection of government information assets and government information systems.

The Defensible Security elements that relate to all IMIT security standards (highlighted in blue in the table below) are: Executive Support, Roles & Responsibilities, Incident Management, Policy (Information Security), Awareness Program/Courses, and Security Governance.

Additional elements specific to the ISS (highlighted in yellow) are: Risk Appetite & Register, Security Assessment, Asset Management, Change Management, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Backup & Retention, Logging & Monitoring, Physical Security & Visible ID, Logical Access, Personnel Security, Defence-in-Depth (endpoints & networks), Vulnerability Management (VM) & Patching, Application Security (AppSec), Program (Information Security), and Information Security (InfoSec) Classification.

Pre-requisites	Directives	Respiration	DNA (Culture)
Executive Support	**Asset** Management	**Backup** & Retention	**Program** (Information Security)
Roles & Responsibilities	**Change** Management	**Logging** & Monitoring	**InfoSec** Classification

Pre-requisites	Directives	Respiration	DNA (Culture)
Crown Jewels	**Incident** Management	**Physical** & Visible ID	**Aware** Program/Courses
Risk Appetite & Register	**BCP**	**Logical** Access	**Security** Governance
Risk Assessment	**DRP**	**Personnel** Security	
Security Assessment	**Incident** Response	**Defense**-in-Depth (endpoints & networks)	
	Policy (Information Security)	**VM** & Patching	
	Vendor Requirements	**AppSec**	

3. RESPONSIBILITY ASSIGNMENT MATRIX (RACI CHART)

R = Responsible; A = Accountable; C = Consult; I = Inform

Information Security Standard Deliverables	**Roles**							
	Information Owner	**Information Custodian**	**Government Chief Information Officer (GCIO)**	**Ministry Chief Information Officer (MCIO)**	**Chief Information Security Officer (CISO)**	**Ministry Information Security Officer (MISO)**	**Supervisor**	**Employee/ Contractor/ Vendor**
Core security policy (ISP)	**I**	**I**	**AR**	**CRI**	**CR**	**CR**	**I**	**I**
Ministry security policy	**CI**	**CI**	**I**	**AR**	**I**	**CR**	**C**	**I**
Organization of information security in government	**R**	**I**	**AR**	**I**	**CR**	**I**	**I**	**I**
Security coordination	**CR**	**I**	**AR**	**CR**	**CR**	**CI**	**R**	**I**

Information Security Standard Deliverables	Roles							
	Information Owner	Information Custodian	Government Chief Information Officer (GCIO)	Ministry Chief Information Officer (MCIO)	Chief Information Security Officer (CISO)	Ministry Information Security Officer (MISO)	Supervisor	Employee/ Contractor/ Vendor
Security roles and responsibilities	**CR**	**RI**	**AR**	**I**	**CR**	**CI**	**RI**	**(R)I**[1]
Appropriate security contacts	**I**	**I**	**AC**	**I**	**CR**	**R**	**I**	**I**
Information security integration in project management	**AR**	**R**	**C**	**I**	**CR**	**CR**	**I**	**(R)I**
Security in new information systems and processing facilities	**AR**	**I**	**CI**	**CR**	**C**	**CR**	**I**	**(R)I**
Related security policies & standards	**RI**	**RI**	**A**	**CI**	**CRI**	**CRI**	**I**	**(R)I**

4. ROLES & RESPONSIBILITIES

See **Section 5.2.3** below.

5. SPECIFICATIONS

5.1. INFORMATION SECURITY POLICIES

The Office of the Government Chief Information Officer (GCIO) is responsible for the Information Security Policy (ISP). Ministries or agencies are responsible for their own information security policies.

5.1.1. Information Security Policy (ISP)

The ISP contains government requirements for the secure delivery of services that provides the assurance of confidentiality, integrity, availability and privacy of government information assets through:

[1] **(R)I** means that contractors & vendors are responsible, and employees are informed.

- 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 information assets;
- Ensuring operational security, protection of networks and the transfer of information;
- Safe-guarding information assets utilized by third parties;
- Reporting information security incidents and weaknesses;
- Creating and maintaining business continuity plans; and
- Monitoring for compliance.

Where standards exist, they are referenced in individual policies. All relevant policies, standards and additional resources appear in **Cheat Sheet to Resources to Enable Information Security** webpage. The Office of the GCIO will issue and revise government standards as needed. Specification and guideline documents may also be included as needed to assist in the interpretation and implementation of a standard.

5.1.2. Ministry or Agency Information Security Policy

Ministries may develop and implement information security policies, standards, specification and guideline documents for use within their organization or for a specific information system or program.

Ministry awareness programs should identify the ISP and ministry developed information security policies to enable employees to be aware of the policies that affect their program areas.

5.1.3. Information Security Policy Review

a) Information Security Policy (ISP) Review

The Office of the Government CIO is responsible for reviewing the ISP, IMIT standards specification and guideline documents on an annual basis. Policy and standards reviews MUST be initiated:

- In conjunction with legislative, regulatory or policy changes that 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; or,
- When associated external agencies (e.g. Information and Privacy Commissioner, National CIO Sub-Committee on Information Protection, RCMP, etc.) issue reports or identify emerging trends related to information security.

b) Ministry or Agency Information Security Policy Review

Ministries/agencies who have developed their own ministry/agency specific information security policies, standards, specification and guideline documents MUST review them **at least** annually. Documented processes MUST be used to develop, review and approve them.

5.2. ORGANIZATION OF INFORMATION SECURITY

5.2.1. Internal Organization

The Office of the Government CIO recognizes that information security is a process. For this process to be effective, executive and management commitment, the active participation of all employees and ongoing awareness programs are needed. To enable this, the management structure needs to be organized to provide guidance on who coordinates the information security activities and what agreements are required.

The internal organization structure required is as follows:

- Executive team;
- Chief Information Security Officer; and,
- Information Security Branch.

a) Executive Team

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.

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

The OCIO has developed an information security program framework, i.e. **Defensible Security**, to provide ministries 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 ISP;
- Monitoring and measuring the implementation of the ISP; and,
- Developing and delivering a program to maintain information security awareness.

b) Chief Information Security Officer (CISO)

Please refer to the **Security Roles and Responsibilities** for more information on this role.

c) Information Security Branch Support

The CISO is the Executive Director of the Information Security Branch (ISB). Information security specialists in the ISB, OCIO, are responsible for:

- Interpreting the ISP to assist in the delivery of business functions;
- Evaluating information security implications of new government initiatives;
- Performing information security risk analysis activities;
- Performing Security Threat and Risk Assessment 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 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.

5.2.2. Security Coordination

a) Security Coordination Across Government

A cross-government information security forum that meets several times a year will provide advice and recommendations for:

- Developing and implementing information security policies, standards, specification and guideline documents;
- 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.

b) Security Coordination Within a Ministry

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

- Determine the information security priorities and requirements of the ministry;
- Communicate the security priorities, requirements and issues to the cross-government information security forum;
- Ensure standards, procedures and processes are developed, documented and implemented to support day-to-day information security activities in compliance with policy;
- Promote information security awareness and education;
- Ensure the Information Incident Management Process is followed for all suspected or actual information incidents; and,
- Follow up on information incidents investigations findings.

5.2.3. Information Security Roles and Responsibilities

The security responsibilities are documented in the job descriptions of the MCIO, MISO and delegated Supervisors. MCIOs, MISOs and delegated Supervisors acknowledge that they have been briefed and understand their responsibilities via their job acceptance letters.

All government employees are required to complete the mandatory annual security training (e.g. IM117) that communicates employee security responsibilities. They agree to their role and responsibilities in information security outlined in the Appropriate Use Policy (AUP) when they sign the Appropriate Use of Government Information and Government Information Technology (IM/IT) Agreement upon hire. Employees should also familiarize themselves with the security responsibilities outlined in published guides/guidelines, e.g. Record Management Guides, Mobile Device Guidelines, Security While Travelling, etc.

a) Responsibilities

Responsibility for security throughout government includes:

- Identifying the Information Owner and Information Custodian responsible for information and information systems;
- Identifying the assets and defining security processes; and,
- Defining authorization levels for access to the information and information systems.

i. 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 to others by the Deputy Minister.

Information Owners have the responsibility and decision-making authority for information throughout its lifecycle. This includes creating, classifying, restricting, regulating and administering its use or disclosure as well as disposal. See the **Security Roles and Responsibilities** for detailed responsibilities for this role.

Information Owners also have the responsibility to:

- Document information security roles and responsibilities for employees in job descriptions, standing offers, contracts, and information use agreements where relevant;
- Review and update information roles and responsibilities when conducting staffing or contracting activities;
- Ensure segregation of duties – see **Section 5.2.4** for more details;
- Ensure information security risks are addressed in projects – see **Section 5.2.6**

- Ensure new information systems or processing facilities have been approved – see **Section 5.2.7** for more details;

To ensure all controls and protection levels are secure by design, Information Owners MUST consult the OCIO and the CISO, or a designate:

- When corporate shared infrastructure and services are part of the business operation infrastructure (e.g. security architecture, policy, standards, and security controls requirements); and,
- When defining the standards and contractual requirements for the procurement of outsourced corporate shared infrastructure and services.

Information Owners can delegate authority to Information Custodians through:

- Formal agreements (e.g. a service level agreement between a Ministry and service provider);
- Memorandums (e.g. a Minister/Deputy Minister memorandum to a service area); or,
- Service descriptions (e.g. service catalogue description).

ii. Information Custodians

See the **Security Roles and Responsibilities** for detailed responsibilities for this role.

Information Custodians MUST also consult the OCIO and the CISO, or a designate when:

- Corporate shared infrastructure and services will be part of the business operations infrastructure; or,
- Procuring outsourced corporate shared infrastructure and services, to ensure the contract with the service provider has all the required security controls and protection defined.

iii. Ministry Chief Information Officer

The responsibilities of the Ministry Chief Information Officer (MCIO) for IM IT administration may be delegated by the Deputy Minister (see Core Policy and Procedures Manual, Chapter 12 – Information Management and Information Technology Management). See the **Security Roles and Responsibilities** for detailed responsibilities for this role.

iv. Ministry Information Security Officer

See **Security Roles and Responsibilities** for detailed responsibilities for this role.

v. 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.

vi. Supervisors

Supervisors are employees with direct reports. See **Security Roles and Responsibilities** for detailed responsibilities for this role. Supervisors MUST also:

- Establish processes to communicate security roles and responsibilities to employees to protect information assets;
- Understand and communicate information security policies and standards to employees;
- Review employee access rights to information resources on a regular basis, especially whenever a new employee is onboarded or when a change in employee roles and responsibilities occurs; and,
- Ensure there are processes to approve and support the use of non-government hardware to conduct government business if use of such hardware is critical to the business. The processes MUST address the requirements for information security, privacy and data ownership.

vii. Employees

Employees MUST be aware of their information security roles and responsibilities. They are responsible for 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. See **Security Roles and Responsibilities** for more information for this role.

viii. Contractors

See **Security Roles and Responsibilities** for more information for this role.

ix. Vendors

See **Security Roles and Responsibilities** for more information for this role.

5.2.4. Segregation of Duties and Responsibilities

a) Segregation of Duties

Information Owners and Information Custodians MUST reduce the risk of disruption to 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 (e.g., automated alerts for unusual/abnormal system activity);
- Requiring that individuals authorized to conduct sensitive operations do not audit the same operations (e.g., ensuring that application system administrators are unable to modify the application or system logs);
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action (e.g. the person granting access to an information system is also not the approver for the access); and,
- Implementing security controls to minimize opportunities for collusion.

Information Owners and Information Custodians should:

- Annually confirm that privileged user controls are limited to the user's job responsibilities through an access analysis; and,
- Confirm through financial risk control reviews and/or independent audits that segregation of duties has been done adequately for critical systems i.e. that no single person is responsible for both the operation and audit of the systems.

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 at least two-person access control to preserve the integrity of the information system. For instance, no same person should be responsible for managing both the operating system of an information system and the applications of the information system.

5.2.5. Appropriate Contacts

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.

A process is in place to ensure contact lists are reviewed and updated at a minimum annually (e.g., part of the Business Continuity Program review).

b) Participation in Security Forums and Professional Associations

The Chief Information Security Officer MUST promote professional certification and membership in professional associations (e.g. CISSP, CISM, CCSP, CISA, ISACA, etc.) for information security specialists throughout government. Employees with security responsibilities MUST maintain their knowledge of information security industry trends, best practices, technology advances and threats or vulnerabilities by:

- Participating several times in a year in information exchange forums regarding best practices, industry standards development, technology advances, threats, vulnerabilities, early notice of potential attacks, and advisories;
- Maintaining and improving knowledge regarding information security best practices by maintaining their membership with a recognized professional association, attending security meetings, security conferences and information sessions; and,
- Creating a support network with other security specialists.

5.2.6. Information Security in Project Management

Information Owners and Information Custodians MUST integrate information security into every phase of the organization's project management methods. This is 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;
- Information security implications are reviewed during all phases of the applied project methodology; and,
- Security roles and responsibilities are defined and allocated to specific roles defined in project management methods.

5.2.7. New Information Systems and Processing Facilities

a) Approval for Information Processing Facilities

Prior to constructing any new information processing facility, 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; and,
- Obtain advice from the Office of the Government Chief Information Officer to ensure adherence to relevant policies, procedures, standards, specifications, and guidelines for physical security of the facility.

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;
- Ensure new and significantly changed information systems undergo certification and accreditation; and,
- Obtain approval from the Office of the Government Chief Information Officer to ensure adherence to relevant Core Policies and Procedures, including the Information Security Policy, and the IMIT security standards.

c) Acquisition of Hardware, Firmware and Software

Prior to acquisition of new hardware, firmware or software, Information Owners, and Information Custodians MUST:

- Ensure new hardware, firmware and software conform to government standards;
- Evaluate compatibility with existing information systems hardware, firmware, and software;

- Consider the reliability of the product as part of the procurement selection process; and,
- Evaluate the need for any additional security measures and the impact on existing security processes.

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

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.

When extenuating circumstances require the use of non-government hardware to conduct government business, employees MUST first obtain supervisor approval to do so.

6. DEFINITIONS/GLOSSARY

The following key words in this document are to be interpreted as described in RFC 2119 (see https://tools.ietf.org/html/rfc2119):

- MAY;
- MUST;
- MUST NOT;
- OPTIONAL;
- RECOMMENDED;
- REQUIRED;
- SHALL NOT;
- SHALL;
- SHOULD; and,
- SHOULD NOT

See **Information Security Glossary** and **Appendix A: Terms and Definitions** for more.

7. SUPPORTING DOCUMENTS

- Defensible Security Framework
- Security Roles and Responsibilities
- Cheat Sheet to Resources to Enable Information Security

- IMIT 6.19 Information Security Standard

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revisions
1.0	2022-01-6	Sharina Gopaldas Johnston	Document creation.

9. CONTACTS

For questions or comments regarding this standard, please contact:

Information Security Branch, Office of the Chief Information Officer
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca

APPENDIX A: TERMS AND DEFINITIONS

There are some word pairs used in the Information Security Standard (ISS) that users have found confusing and require clarification. These word pairs are defined here, apart from the Glossary (Appendix C) because they do apply to the ISS overall and are used throughout.

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

"**Information Custodians**" maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. In contrast, information custody means having physical possession of information without necessarily having responsibility for the information.

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

Standards vs Guidelines – "**Standards**" refer to industry specific standards, government standards and standardized process documents developed to support a specific policy or requirement. "**Standards**" are industry-approved specifications for quality that can be measured against. Organizations can exceed the standards but should not fall below them. "**Guidelines**" refer to recommendations, best practice or support documents and processes that help with the interpretation and implementation of a specific policy or requirement. "**Guidelines**", where they are provided, serve to assist someone and offer some direction.

Exceptions vs Exemptions – "**Exceptions**" refer to specific cases where a certain requirement does not apply. Where for certain reasons a Ministry or a program area cannot comply with a specific requirement, they must request an **Exemption**. The request submission must be accompanied by a completed Security Threat and Risk Assessment and Privacy Impact Assessment. Exemption requests follow a stringent review process by the Office of the Government Chief Information Officer.

Specifications vs Guidelines – "Specifications" refer to detailed requirements not included in the "Standards", guidance on how the standard links to Defensible Security, and the roles and responsibilities for the deliverables of the standard.