1. PURPOSE

To provide a framework that helps government organizations meet their goals to protect government information and technology assets. This standard enables the comprehensive Information Security Program that supports Chapter 12 of the Core Policy and Procedures Manual. This program is headed by the Chief Information Security Officer, who is the Executive Director of the Information Security Branch.

2. DESCRIPTION

The IMIT 6.19 Information Security Standard (ISS) provides a structured approach to identifying the broad spectrum of information security activities in the life cycle of information systems. This standard also incorporates a risk-based approach to information security, i.e. the use of Security Threat and Risk Assessments to consider business process and government service delivery implications and technology implications. It also requires communications strategies including employee information security awareness programs. Version 2.0 of the IMIT 6.19 ISS reflected the Information Security Policy V4.1, a cross-government policy for information security that was based on the International Standardization Organization (ISO) 27002:2013 standard for information security management.

Version 3.0 of the IMIT 6.19 ISS uses a new template for the standard and has some updates such as clarification of language, removal of references to retired IM/IT standards and updated hyperlinks. In addition to this standard, the new **6.19 Information Security Standard (ISS) Specification** document provides detailed requirements. The specifications outlined in the **6.19 ISS Specification** document MUST be followed in conjunction with this standard.

3. AUTHORITY

- Core Policy and Procedures Manual (CPPM) - Chapter 12: Information Management and Information Technology Management.
- Information Security Policy (ISP).

4. APPLICATION / SCOPE

The ISS applies to core government. Contracted service providers conducting business on behalf of government MUST comply with the ISS (or demonstrate compliance with ISO 27002:2013) and the other IM/IT Standards. See **Section 7** below for a list of references and hyperlinks.

Exemptions from an IM/IT Standard may be granted subject to the approval of the Government Chief Information Officer (Government CIO). An exemption request and supporting documentation for the business need MUST be submitted to the Government CIO

for consideration of the exemption request. See the **6.19 ISS Specification**, **Appendix A** for more details.

5. REQUIREMENTS

5.1. Information Security Policies

All information security policies MUST be published and communicated to all employees and relevant external parties.

5.1.1. Information Security Policy

The Office of the Government CIO is responsible for establishing, issuing and monitoring the Government Information Security Policy (ISP), processes and practices that will assist Ministries in delivering secure services. See **6.19 ISS Specification** **Section 5** for more details.

5.1.2. Ministry or Agency Information Security Policy

Ministry/agency developed information security policies can exceed but MUST NOT conflict with Government ISP and standards established by the Office of the Government CIO. See **6.19 ISS Specification** **Section 5** for more details.

5.1.3. Information Security Policy Review

The ISP and ministry/agency information security policies MUST be reviewed on an annual basis and updated when required to ensure they remain current with evolving business needs, emerging risks and technology changes. See **6.19 ISS Specification** **Section 5** for more details.

5.2. Organization of Information Security

5.2.1. Internal Organization

Executive MUST provide strong leadership support by setting the direction. The management structure needs to-be organized to coordinate the information security activities to support the implementation of the requirements in the ISP. See **6.19 ISS Specification** **Section 5** for more details.

5.2.2. Security Coordination

Implementation of information security activities across government MUST be coordinated by the Office of the Government CIO to ensure that information security activities are carried out in a timely manner to resolve security issues. See **6.19 ISS Specification** **Section 5** for more details.

5.2.3. Information Security Roles and Responsibilities

Information security roles and responsibilities for information and information systems MUST be defined, documented and communicated to ensure employees are

informed of their information roles and responsibilities. See **6.19 ISS Specification Section 5** for more details.

5.2.4. Segregation of Duties and Responsibilities

Duties and areas of responsibility MUST be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of information systems. See **6.19 ISS Specification Section 5** for more details.

5.2.5. Appropriate Contacts

Appropriate contacts shall be maintained with:

a) Local law enforcement authorities, emergency support employees to facilitate coordination with and timely response from outside authorities during information security incidents or investigations; and,

b) Specialist security forums and professional associations to promote and further employee knowledge on:
   - information security industry trends;
   - best practices;
   - new technologies; and,
   - threats or vulnerabilities.

See **6.19 ISS Specification Section 5** for more details.

5.2.6. Information Security in Project Management

Information security risks MUST be identified and addressed throughout a project lifecycle. See **6.19 ISS Specification Section 5** for more details.

5.2.7. New Information Systems and Processing Facilities

The establishment of a new or significantly modified information system or processing facility MUST be formally reviewed before it is approved to ensure there are adequate security controls implemented for its secure operation. See **6.19 ISS Specification Section 5** for more details.

5.3. Mobile Computing and Teleworking

Please see:

a) Mobile Device Security Standard (at: IM/IT Standards) and the Mobile Device Guidelines for BC Public Employees for mobile computing.

b) Core Policy and Procedures Manual (CPPM) Chapters 12 & 15, Appropriate Use Policy, BC PSA's Teleworking Agreement, How to Protect Your Home Computer Tip Guide and the Flexible Work in the BC Public Service FAQ for guidance on teleworking.

5.4. Human Resource Security

Please see:

a) BC Public Service Agency (BCPSA) HR Policy #14 for employee screening.
b) CPPM Chapter 6 and Government Services Agreement (GSA) Schedule G for contractor screening.
c) Appropriate Use Policy and BCPSA Onboarding process for information and information system security responsibilities and terms and conditions of employment.
d) BCPSA Accountability Framework for Human Resource Management Appendix A for supervisory responsibilities in a security investigation.
e) The Privacy Breaches website for responsibilities and actions by all employees and supervisors in the event of a privacy or information incident.

5.5. Asset Management

Please see the IMIT 6.23 Asset Management Security Standard (at: IM/IT Standards).

5.6. Access Control

Please see the IMIT 6.24 Access Control Security Standard (at: IM/IT Standards).

5.7. Cryptography

Please see the IMIT 6.10 Cryptographic Standards for Information Protection (at: IM/IT Standards).

5.8. Physical and Environmental Security

Please see the IMIT 6.26 Physical and Environmental Security Standard (at: IM/IT Standards).

5.9. Operations Security

Please see the IMIT 6.27 Operations Security Standard (at: IM/IT Standards).

5.10. Communications Security

Please see the IMIT 6.28 Communications Security Standard (at: IM/IT Standards).

5.11. System Acquisition, Development and Maintenance

Please see the IMIT 6.29 Systems Acquisition, Development and Maintenance Security Standard (at: IM/IT Standards).

5.12. Supplier Relationships (and Cloud Computing)

Please see the IMIT 6.30 Supplier Relationships (and Cloud Computing) Security Standard (at: IM/IT Standards).

5.13. Information Security Incident Management

Please see the IMIT 6.31 Information Security Incident Management Standard (at: IM/IT Standards).

5.14. Information Security Aspects of Business Continuity Management

Please see the IMIT 6.32 Information Security Aspects of Business Continuity Management Standard (at: IM/IT Standards).

5.15. Compliance

Please see the IMIT 6.33 Compliance Security Standard (at: IM/IT Standards).

6. DEFINITIONS/GLOSSARY

See **6.19 ISS Specification** **Section 6** for more information.

7. SUPPORTING DOCUMENTS

See **6.19 ISS Specification** **Section 7** for details.

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revisions
2.0	2019-01	Daniel Surdu	Approved by CIO & published.
3.0	2022-06	Sharina Gopaldas Johnston	New template, removal of references to retired standards & policies, hyperlinks update, addition of references to relevant alternative security instruments that replace the retired standards, removal of standard details to specification document and language clarification for comprehension.

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