Document Version: 2.0
Effective Date: September 2019
Last Reviewed: August 2024

1. Purpose

To establish the requirements to incorporate security measures into the processes in the management of the lifecycle of an information system.

This standard supplements the IMIT 6.27 Operations Security Standard by providing additional guidance on integrating information security into the processes for the acquisition or creation, modification, implementation, and expansion of information systems and applications.

The IMIT 6.29 System Acquisition, Development, and Maintenance Security Specifications document provides detailed specifications for this standard. Both this standard and the specifications MUST be followed.

2. Application

This IMIT 6.29 System Acquisition, Development, and Maintenance Security Standard applies to:

- Ministries, agencies, boards, and commissions (referred to as ministries in this standard) who are subject to the Core Policy and Procedures Manual.
- Contracted service providers and any other third-party entity conducting business or managing information or information assets on behalf of the B.C. government.

3. Requirements

3.1 Security requirements of information systems

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.1.1 Identify information security requirements as part of business requirements for new information systems or enhancements to existing information systems.

3.1.2 Ensure information system development or acquisition activities are conducted following documented standards and procedures.

3.1.3 Implement sufficient controls to mitigate the risk of information error, misuse, or loss from information systems.

3.1.4 Document and maintain system security plans for the information systems.

3.1.5 Protect information in electronic commerce information systems from unauthorized disclosure and modification, fraudulent activity, and contract dispute.

3.1.6 Protect the authenticity, integrity, and confidentiality of digital documents.

3.1.7 Ensure information systems with online transactions use security controls equal to the value and sensitivity of the online transaction information.

3.1.8 Ensure information systems used for processing payment card transactions or connected to payment card transaction processing systems are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

3.2 Security in development and support processes

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.2.1 Establish and maintain policies, standards, guidelines, and best practices for the secure development of software and systems and apply them consistently to all internally developed software and systems throughout the development lifecycle of information systems.

3.2.2 Ensure secure programming techniques are used for new developments and when standards applied to the development of the code being reused may not be known or are not consistent with current best practices.

3.2.3 Control changes to software through formal change control procedures to ensure information systems are not compromised from unauthorized changes to software.

3.2.4 Review and test information systems when operating systems changes occur to ensure the information systems are not disrupted or compromised by the changes.

3.2.5 Control, document, and limit modifications to commercial-off-the-shelf (COTS) software to essential changes to reduce the risk of information system functionality loss.

3.2.6 Implement a software update management process for applying vendor-supplied patches and updates.

3.2.7 Ensure information security is designed into all architectural layers of information systems by requiring secure information system engineering principles and procedures to be applied to:

1. In-house information system engineering activities.
2. Outsourced information systems through contracts and other binding agreements.

3.2.8 Establish and protect secure development environments for system development and integration efforts to ensure the security of information is protected during the entire system development lifecycle.

3.2.9 Apply controls to secure outsourced information system development to ensure the information system performs as expected and meets security requirements.

3.2.10 Conduct security functionality testing during the development process.

3.2.11 Establish and document acceptance criteria for new information systems, upgrades, or new versions as part of the system development and acquisition process.

3.2.12 Complete security certifications for new information systems, upgrades, or new versions.

3.2.13 Complete system accreditation for new information systems, upgrades, or new versions.

3.3 Correct processing in applications

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.3.1 Validate data input to an information system to ensure it is correct and appropriate to maintain information integrity in the information systems.

3.3.2 Perform internal processing checks to minimize the risk of processing failures or deliberate acts leading to a loss of integrity.

3.3.3 Use message integrity controls for information systems to protect the authenticity of the message content where maintaining message integrity is a security requirement.

3.3.4 Validate data output from an information system to ensure the processing of stored information is correct and appropriate to the circumstances.

3.4 Test Data

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.4.1 Protect and control test data when using production data for testing with the same procedures used for data in the production environment to protect information from unauthorized access or use.

4. Supporting documents

IMIT 6.27 Operations Security Standard

IMIT 6.29 System Acquisition, Development, and Maintenance Security Specifications

Payment Card Industry Data Security Standard (PCI DSS)

5. Definitions

Information Security Glossary

6. Authority

Core Policy & Procedures Manual (CPPM)

Information Security Policy

7. Revision history

This standard is reviewed annually and updated as needed.

Version	Revision Date	Author	Description of Revisions
2.0	August 2024	S. Gopaldas Johnston	Document format and layout update to new template; move of detailed requirements to specifications document; clarification of language.

8. Contact

For questions regarding this standard, contact:

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