1. Purpose

To identify the minimum technical security requirements for secure government applications.

The standard describes the minimum controls for secure software development and maintenance, and for the protection of B.C. government applications, including web and mobile applications. A security threat and risk assessment may identify additional application security requirements.

This standard supplements the IMIT 6.27 Operations Security Standard and the IMIT 6.29 System Acquisition, Development, and Maintenance Security Standard. The IMIT 6.14 Application and Web Security Specifications document provides detailed specifications for this standard. Both this standard and the specifications MUST be followed.

2. Application

This IMIT 6.14 Application and Web Security Standard applies to:

- All applications developed for the B.C. government.
- 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 Secure software development

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

3.1.1 A security threat and risk assessment is performed at every stage of the software development life cycle (SDLC) process for every application.

3.1.2 All security controls specific to developing and deploying the software application are described in the system security plan[1].

3.1.3 A software development life cycle (SDLC) process for software development and the security of the code is assessed at every stage of the SDLC.

3.1.4 Applications for mobile devices have digital signatures.

Secure coding

3.1.5 Custom code, that is an application developed by or on behalf of B.C. government, is developed based on secure coding practices to minimize attack opportunities.

3.1.6 Insecure application programming interfaces (APIs) are NOT used.

3.1.7 For custom code that accesses databases, the custom code contains security controls to limit unnecessary and unauthorized database exposure.

Secure code review requirements

3.1.8 Custom code is reviewed, tested, and remediated for coding vulnerabilities before the code is released.

3.1.9 Code reviews are performed by automated means, or if manually, by development team member(s) other than the original code author.

3.1.10 An application is reviewed for vulnerabilities at a frequency dictated by the sensitivity of the information it will collect, process, or transmit, or its criticality to business operations.

[1] See IMIT 6.29 System Acquisition, Development, and Maintenance Security Standard for more information on the system security plan.

3.2 Secure software maintenance

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

Security patches

3.2.1 The latest security patches for system components and software are applied.

3.2.2 A risk-based approach is used to prioritize the installation of security patches.

Security vulnerability management

3.2.3 Security vulnerabilities are prioritized and recorded.

3.2.4 All patch management activities are logged in the system security plan for the associated information system.

3.3 Protection of the production environment

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

3.3.1 Production environments are segregated from non-production environments.

3.3.2 Separation of duties is enforced in the software development cycle.

Attack prevention

3.3.3 Automated scanning scripts for code review are verified regularly.

3.3.4 A public-facing web application is isolated from the back-end networks and information systems.

Attack detection

3.3.5 Logging for all applications is enabled to support enable detection of attacks and system faults. The logs must contain sufficient detail to enable proper investigation into incidents.

4. Supporting documents

IMIT 6.11 Security Threat Risk Assessment Standard

IMIT 6.14 Application and Web Security Specifications

IMIT 6.18 Information Security Classification Standard

IMIT 6.29 System Acquisition, Development, and Maintenance Security Standard

5. Definitions

Information Security Glossary

6. Authority

Core Policy and Procedures Manual

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	Transfer to new template. Content updates and additions.
1.3	April 2015	C. Brown	Add: Effective date info, Appendix D - Assessment Guidelines, and Document Header / Footer details.
1.2	November 2012	H. Lee	Revised to accommodate the comments from NR sector, DataBC and MoH.
1.1	November 2012	H. Lee	Revised to accommodate the comments from ASRB members.
1.0	October 2012	C. Brown	First release.

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