Document Version: 5.0
Effective Date: November 2022
Last Reviewed: August 2024

# 1. Purpose

To identify the information transfer requirements to safeguard electronic communication across government.

This standard identifies the information security requirements for network and communication services, including wireless networks. It ensures security controls and practices are implemented and documented to preserve network security as well as ensuring they align with defensible security principles.

The IMIT 6.28 Network and Communications Security Specifications document provides detailed specifications for this standard. Both this standard and the specifications MUST be followed.

**Note:** This standard includes the requirements from the IMIT 5.09 Wireless Local Area Network Security Standard, which is now retired.

# 2. Application

This IMIT 6.28 Network and Communications Security Standard applies to:

- All government organizations (ministries, public agencies, boards, and commissions) who are subject to the Core Policy and Procedures Manual.
- Service providers and any other entity conducting business or managing the B.C. government's information on their behalf.

# 3. Requirements

## 3.1 Network controls

Ministries and OCIO MUST:

3.1.1 Implement and document network security controls and network security management practices to maintain network security.

3.1.2 Restrict access to network devices via central authentication and automated updates.

3.1.3 Establish configuration controls to safeguard the confidentiality and integrity of data passing across networks.

3.1.4 Select controls based on the information security classification determined by the Information Owners, and applicability to the network technology.

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

3.1.6 Regularly perform configuration status accounting to ensure that configuration baselines reflect actual device configuration.

3.1.7 Where required by information security classification and risk assessment, transmit information using only a secured path. Secured paths for information transmission MUST use controls such as:

- Data, message, or session encryption, such as Secure Shell (SSH), Secure Socket Layer (SSL), or Virtual Private Network (VPN) tunnels.
- Systems to detect tampering.

## 3.2 Wireless Local Area Networking

Ministries and OCIO MUST:

3.2.1 Ensure wireless local area network (WLAN) access points are authorized by the Office of the Chief Information Officer for attachment to the government network.

3.2.2 Ensure WLANs use the controls specified by the Chief Information Security Officer (CISO) 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 using filters, firewalls, or proxies.
- Port-based access control (for example, use of 802.1x technology).

3.2.3 Apply appropriate security controls for wireless networks that handle and transmit Protected A, B, or C classified information. Security control examples are VPN tunnel technology, desktop terminal services (DTS) technology, intrusion prevention/detection systems, firewalls, media access control (MAC), and address filtering.

## 3.3 Logging, monitoring, and detection

Ministries and OCIO MUST:

3.3.1 Monitor and log network activities. Ministries SHOULD use corporate Security Incident and Event Management (SIEM) solutions and ensure effective logging and monitoring is done.

## 3.4 Network service agreement

Ministries and OCIO MUST:

3.4.1 Establish configuration controls to safeguard the confidentiality and integrity of data passing across government networks.

3.4.2 Include the requirement for risk assessments in service level agreements for all networks.

3.4.3 Ensure all network service arrangements have a documented network service agreement in place that specifies security features.

3.4.4 Ensure all network service agreements include the requirement that the network service provider's security controls are regularly monitored and have annual audits completed.

## 3.5 Segregation based on risk and business connectivity requirements

Ministries and OCIO MUST:

3.5.1 Segregate groups of information services, users, and information systems on networks.

3.5.2 Restrict device access to the network via central authentication.

3.5.3 Have automated updates enables on devices connected to the network.

3.5.4 Establish configuration controls to safeguard the confidentiality and integrity of data passing across public networks.

3.5.5 Use security gateways, if possible, to verify the trustworthiness of devices attempting to connect to the network (for example, VPN quarantine systems, network switch isolation, and admission control systems).

## 3.6 Routing controls

Ministries and OCIO MUST:

3.6.1 Ensure networks have routing controls to ensure that device connections and information flows do not breach the access control policy of the information system.

3.6.2 Ensure network routing controls include safeguards to prevent unauthorized access or bypassing of security control points.

## 3.7 Communication security controls

Ministries and OCIO MUST:

3.7.1 Implement procedures to protect transferred information from interception, copying, modification, misrouting, and disposal.

3.7.2 Implement anti-malware detection and protection controls.

## 3.8 Electronic messages

Electronic messages created, compiled, sent, or received on government information systems are records of the government and are the property of the B.C. government.

Ministries and OCIO MUST:

3.8.1 Manage electronic messages per the Information Management Act and related regulations, policies, standards and procedures.

3.8.2 Ensure electronic messages are subject to the access and the protection of privacy provisions of the Freedom of Information and Protection of Privacy Act.

## 3.9 Exchange agreements

Ministries and OCIO MUST ensure:

3.9.1 Information and software exchange agreements between the B.C. government and other organizations address the secure transfer of information between parties.

3.9.2 Legal counsel reviews exchange agreements for the B.C. government before the agreements are signed.

## 3.10 Confidentiality agreements

Ministries and OCIO MUST:

3.10.1 Implement and regularly review a confidentiality agreement reflecting organizational requirements for handling information.

3.10.2 Review and annually update confidentiality requirements.

## 4. Supporting documents

IMIT 6.18 Information Security Classification Standard

IMIT 6.28 Network and Communications Security Specifications

## 5. Definitions

Information Security Glossary

## 6. Authority

Core Policy and Procedures Manual (CPPM)

Information Security Policy

## 7. Revision history

| Version | Revision Date | Author | Description of Revisions |
|---|---|---|---|
| 5.0 | August 2024 | K. Petrosyan | New template, updated content. Includes requirements from the IMIT 5.09 WLAN Security Standard |
| 4.1 | February 2012 | C. Lyons | |

## 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