Document Version: 3.1
Effective Date: March 2017
Last Reviewed: August 2024

1. Purpose

To define minimum security requirements for B.C. government-issued mobile devices and the platform that will be used to manage these mobile devices to protect government information.

The IMIT 6.15 Mobile Device Management Security Specifications document provides detailed specifications for this standard. Both this standard and the specifications MUST be followed.

2. Application

For this standard, mobile devices include only smartphones, tablets, and Mac laptops. Windows laptops and other peripheral devices[1] are excluded from the scope of this standard.

The IMIT 6.15 Mobile Device Management Security Standard applies to:

- Ministries, agencies, boards, and commissions (referred to as ministries in this standard) that 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.
- All mobile devices used to conduct government business.

[1] Mobile peripheral devices and companion devices require a parent device (like a smartphone) to fully operate. Examples include smart watches (Apple Watch, Samsung Galaxy Watch) and portable Wi-Fi hotspot devices.

3. Requirements

3.1 Mobile device planning, acquisition, and requirements

The OCIO MUST ensure:

3.1.1 Security controls on mobile devices follow B.C. government IM/IT policies and standards to protect information.

3.1.2 Mobile devices used for government business are enrolled and managed by the OCIO mobile device management system.

3.1.3 Information security risks related to mobile devices and their use for government work are assessed and managed.

3.1.4 Encryption is configured and enforced on mobile devices.

3.1.5 Use of removable storage is blocked on mobile devices.

Ministries, in collaboration with the OCIO, MUST:

3.1.6 Ensure all mobile devices are approved by the OCIO.

3.1.7 Update mobile devices to the latest supported operating system version.

3.1.8 Inventory mobile devices regardless of their enrollment in the OCIO mobile device management system.

Ministries MUST:

3.1.9 Immediately identify and report misplaced, lost, or stolen mobile devices, regardless of value.

3.1.10 Ensure that contractor mobile devices used to conduct government business are managed and comply with all device management policies.

3.1.11 Ensure that contractors using government-issued mobile devices comply with B.C. government policies, standards, and contracts governing their provisioning and operation.

3.2 Design, development, testing, and management

The OCIO MUST:

3.2.1 Ensure that the OCIO mobile device management system platform has the capability for securely managing mobile devices.

3.2.2 Ensure that the OCIO mobile device management system follows the change management process for any changes made to a mobile device configuration and the OCIO mobile device management system. This includes changes being tested and authorized before implementation in production systems.

3.2.3 Review the system configuration for the OCIO mobile device management system annually.

3.3 Implementation, operations, and disposition

The OCIO MUST:

3.3.1 Develop, maintain, and publish documentation on the OCIO mobile device management system.

3.3.2 Decommission enrolled mobile devices no longer on the approved list within 90 days (see Mobile Device Selection List and Procurement Information for approved list information).

Ministries MUST:

3.3.3 Securely erase data on mobile devices before issuing device to new users.

3.3.4 Configure[2] mobile devices not enrolled in the mobile device management service to prevent malicious attacks.

3.3.5 Dispose of mobile devices (and any removable storage media used with the device) by following the Disposal Handbook.

[2] Examples of configurations to improve mobile device security include installing anti-malware applications, enabling security settings like lock screen and password, and only allowing applications downloads from official stores.

3.4 Limited circumstances

Ministries MUST:

3.4.1 Consult with the OCIO before using an unapproved mobile device for government business.

3.4.2 Submit a modification request to the OCIO for modifications to the default OCIO mobile device management configuration profile.

4. Supporting documents

Core Policy and Procedures Manual (CPPM) Chapter L: Loss Reporting
Disposal Handbook
IMIT 5.10 Critical Systems Standard
IMIT 6.10 Cryptographic Security Standard
IMIT 6.11 Security Threat Risk Assessment Standard
IMIT 6.19 Information Security Standard
IMIT 6.24 Access Control Security Standard
IMIT 6.28 Communications Security Standard
Information Incident Management Policy

5. Definitions

Information Security Glossary

6. Authority

Core Policy and 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
3.1	August 2024	J. Hatherly	Minor content changes, transfer to new template, rename standard, editing for plain language.
3.0	November 2021	D. Surdu & S. Gopaldas Johnston	Rewrite, removal of end-user security advice to Mobile Device Guidelines, incorporation of security controls from the 6.20 Mobile Computing Security Standard (retired November 2021)
2.0	January 2018	M. Cook	Rewrite, addition of contractor language, 90-day removal & more. Includes updates from ASRB review.
1.1	March 2017	B. Dari	Minor updates.

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