



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.

This document provides detailed security specifications to support the [IMIT 6.15 Mobile Device Management Security Standard](#). Both the standard requirements and these specifications MUST be followed.

2. Resources

Appropriate Use Policy	High-level requirements for accessing and managing government information and using information technology resources.
Defensible Security Framework	Critical security controls (assessment and tools).
IMIT 6.15 Mobile Device Management Security Standard	Corresponding standard for these specifications.
Information Security Glossary	List of information security terms and definitions.
Knowledge Base - My Service Portal 	Knowledge base for corporate mobile devices on OCIO My Service Centre.
Mobile Device Guidelines for BC Public Service Employees	Guidance for government employees on the use of their mobile devices given current legal requirements, government policy, and best practices.
Mobile Device Management Service (MDMS) 	An overview of the mobile device management service including its features, approved mobile devices, and enrollment information.
Tip Sheet for Work-Related, Government-Approved Foreign Travel	Guidance for protecting government information stored on mobile devices while travelling.

3. Specifications

3.1 [Mobile device planning, acquisition, and requirements](#)

3.2 [Design, development, testing, and management](#)

3.3 [Implementation, operations, and disposition](#)

3.4 [Limited circumstances](#)

3.1 Mobile device planning, acquisition, and requirements

The OCIO MUST ensure:

3.1.1 Mobile devices—specifically, their operating systems and enhancements—are securely configured and deployed per the following B.C. government policies and standards.

1. [Information Security Policy](#)
2. [IMIT 6.10 Cryptographic Security Standard](#)
3. [IMIT 6.24 Access Control Security Standard](#)
4. [IMIT 6.28 Communications Security Standard](#)

3.1.2 Mobile devices capable of connecting to a data network or storing data are managed and enrolled into the OCIO mobile device management system before they are used to process, access, or store confidential B.C. government information. (See [Limited circumstances](#) for exceptions to this requirement.) This includes ensuring that:

1. Any mobile device that has not been in contact with the OCIO mobile device management system for 60 days is removed from the system and its access to government networked resources blocked.
2. Data on mobile devices is protected and classified following the [IMIT 6.18 Information Security Classification Standard](#).

3.1.3 An assessment to identify and manage critical and high security risks is completed for:

1. Each new mobile device that is to be approved, if the device differs in a way that could present a new or increased risk by its type, make, model, and device security features.


2. Each approved mobile device's major operating system releases that introduce significant change in function/feature.
 3. The OCIO mobile device management system itself and its upgrades.
- 3.1.4 Mobile devices are configured and enforced for encryption for all storage on enrolled mobile devices. The cryptographic controls must meet the minimum requirements of the [IMIT 6.10 Cryptographic Security Standard](#).
- 3.1.5 Mobile devices are configured to block removable storage, including SD cards, USB flash drives, and external hard drives.

Ministries, in collaboration with the OCIO, MUST ensure:

- 3.1.6 Mobile devices are OCIO-approved. On the [Mobile Device Selection List and Procurement Information](#) page, see Approved Mobile Devices and Operating Systems for the list of approved mobile devices.
- 3.1.7 Any mobile device that cannot be updated to the latest operating system version is replaced with an OCIO-approved device within 90 days.
- 3.1.8 Changes or updates made to government-issued mobile devices that alter their original inventory information are documented, including:
1. Reassignment or disposal
 2. Operating system change (for example, Windows to Linux)
 3. Function change (for example, emergency phone to smartphone)

For ministry inventories of mobile devices that are not enrolled in the OCIO mobile device management system, the information captured in the inventory for mobile devices must meet the minimum requirements listed in the [IMIT 6.23 Asset Management Security Specifications](#), Asset categories, under Mobile devices (including tablets).

Ministries MUST:

- 3.1.9 Identify and report lost or stolen mobile devices immediately, regardless of value, following the [Core Policy and Procedures Manual \(CPPM\) Chapter L: Loss Reporting](#) and the [Information Incident Management Policy](#). Reports of lost or stolen mobile devices must be reviewed regularly to identify enhancements to security awareness programs and compliance programs.
- 3.1.10 Ensure contractor mobile devices used to conduct government business:
1. Are kept updated to the latest operating system version.
 2. Are enrolled in the OCIO mobile device management system as a contractor. Once enrolled, these devices follow the same mobile device management rules and policies as government-issued mobile devices.
 3. Only store B.C. government data within the applications managed through the OCIO mobile device management system, as required by the [Mobile Service: BYOD Terms of Use](#). 
 4. Have confidential government data removed from the contractor's device upon contract termination.
 5. Have Microsoft Defender for Endpoint installed on Android-based devices.

3.2 Design, development, testing, and management

The OCIO MUST ensure:

- 3.2.1 The OCIO mobile device management system platform has the required capabilities for secure management of mobile devices. At minimum, the mobile device management system MUST:
1. Provide asset management capabilities to ministries for enrolled mobile devices by capturing the following inventory information, at minimum:
 - a. Assigned user identity
 - b. Manufacturer
 - c. Device make and model
 - d. Operating system version
 - e. Apps/applications/software installed

- f. Device status
 - g. Last contact time
 - h. Enrollment
- 2. Encrypt data in transit and at rest and meeting minimum cryptographic controls following the [IMIT 6.10 Cryptographic Security Standard](#).
- 3. Follow independent security assurances for the OCIO mobile device management system to meet legal or regulatory requirements, like the Payment Card Industry Data Security Standard (PCI DSS) and B.C. government policies and standards; for example, the [IMIT 5.10 Critical Systems Standard](#).
- 4. Monitor and log:
 - a. Attempts to tamper with the mobile device operating system and blocking them.
 - b. Vulnerable systems. This refers to mobile devices with operating systems that are no longer supported by the vendor for identification and removal from the OCIO mobile device management system.
- 5. Enable application of corporate and ministry level policies.
- 6. Deny the enrollment of unapproved mobile devices, including those that are jail-broken or rooted.
- 7. Configure and enforce access controls such as screen locks and PINs/passwords on all enrolled mobile devices.
- 8. Allow for remote management of all enrolled mobile devices; for example, remote locking, PIN/password reset/change, and secure data erasure of the device.
- 9. Push out operating system and pre-installed standard apps/applications/software patch updates to all enrolled mobile devices.
- 10. Install and update Microsoft Defender for Endpoint on enrolled mobile devices.
- 11. Support multi-factor authentication.

12. Maintain and enforce blocklist of apps/applications/software and block the installation of blocklisted apps/applications/software.
13. Support and enable device restrictions to limit device functionality.
14. Push out compliance policies for:
 - a. Device and OS configuration settings that follow B.C. government policies and standards.
 - b. Password requirements that follow the [IMIT 6.24 Access Control Security Standard](#). If the password authentication on mobile devices cannot meet the complex password requirements found in the [IMIT 6.24 Access Control Standard](#) for government, both a minimum password of at least 6 characters AND an external two-factor authentication or an approved biometric technology (see Table 1) MUST be used on mobile devices.

Table 1: Biometric Technology for Mobile Device Manufacturer's Operating System

Biometric Technology	Apple (iOS)	Samsung (Android)
Fingerprint scanners	Approved	Approved
Facial recognition	Approved	Not approved

- c. Activation of the lock screen on mobile devices after an idle duration that doesn't exceed 15 minutes. Essential applications (like voice command or maps) may remain unlocked to use.
- d. Removing blocklisted apps/applications/software from the enrolled mobile devices.

3.3 Implementation, operations, and disposition

The OCIO MUST:

- 3.3.1 Develop, maintain, and publish current and accurate documentation for mobile device management for:
 1. Ongoing support and operations, like incident management.

2. Operating procedures and responsibilities that maintain the security of mobile devices.

3.4 Limited circumstances

Ministries MUST:

3.4.1 Complete the following before use of an unapproved mobile device:

1. Complete a security threat and risk assessment for the mobile device to ensure that its use does not pose an unacceptable security risk or conflict with OCIO strategic objectives.
2. Request an [exemption](#) to the IMIT 6.15 Mobile Device Management Security Standard from the OCIO to use an unapproved mobile device. If approved, ministries are expected to inventory, track, and manage the unapproved devices that have received exemptions. Unapproved mobile devices may be allowed for temporary use when:
 - a. There are technical limitations. For example, if there is no mobile device management software agent available or the OCIO mobile device management software agent cannot be installed on the mobile device due to its lack of technical capability. These devices MUST be replaced with an approved mobile device within 90 days.
 - b. Mobile devices with the technical capability to access data networks (like Wi-Fi) and store information but are not configured with a cellular data plan.

Note: No exemption is required for mobile devices that only function as:

- Phone: Only used for voice phone calls (not used for Internet access or applications accessing B.C. government data).
- Kiosk: Mobile devices that do not store or have any access to confidential government information may be used as kiosk or public display devices.
- GPS or emergency phone. These mobile devices MUST NOT have:
 - Cellular data network access plans configured.
 - Wi-Fi data network access configured.
 - Access to any confidential information.

3.4.2 Submit modification requests for the default OCIO mobile device management configuration profile to the OCIO. For example, adjusting access controls (like password and screen lock settings) to meet business requirements to protect confidential government information.

4. Revision history

These specifications are reviewed annually and updated as needed.

Version	Revision Date	Author	Description of Revisions
1.2	August 2024	J. Hatherly	Minor technical updates, new template, rename document, and edit for plain language.
1.1	November 2022	S. Gopaldas Johnston	Replaced reference to iPhone X with Apple and added reference to Samsung Android facial recognition technology. Style guide edits for plain language and improved accessibility.
1.0	November 2021	S. Gopaldas Johnston	New release.

5. Contact

For questions regarding these specifications, contact:

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