## 1. PURPOSE

To establish the baseline security controls that must be applied for the management of mobile devices used for government work that support the Defensible Security principles for the protection of government confidential information.

## 2. DESCRIPTION

This standard was created in response to the BC Auditor General's report on the management of mobile devices in Government. It defines the framework of minimum-security requirements for these mobile devices issued by Government and the platform that will be used to manage these mobile devices. This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) (published here: IM/IT Standards).

## 3. AUTHORITY

Core Policy and Procedures Manual – Section 12: Information Management and Information Technology Management and Section 15: Security.

## 4. APPLICATION / SCOPE

This standard is for ensuring that the platform used to manage mobile devices in government will help ensure secure mobile device use and protect confidential (personal and/or sensitive) information based on current available technology capabilities. It also applies to mobile devices used for government business and are capable of storing confidential (personal and sensitive) information.

## 5. REQUIREMENTS

### 5.1. Mobile Device Planning, Acquisition & Requirements:

5.1.1. Mobile devices are only to be issued by the Province of British Columbia when there is a business reason for doing so, and in accordance with corporate standards.

5.1.2. Mobile devices used for government business MUST have adequate security controls enforced by a BC Government **Enterprise Mobility Management system** (e.g. the system used in the Mobile Device Management (MDM) Service).

5.1.3. The MDM **Service Owner** MUST ensure the new mobile devices or operating system (**OS**), and enhancements to existing devices are compliant with the Information Security Policy and IMIT standards. See the **Mobile Device Security Supplemental (MDSS) 2.1** for more details. The Office of the Chief Information Officer (**OCIO**) Device Services is the OCIO MDM Service Owner.

5.1.4. The OCIO MDM Service Owner MUST:

a) Complete a Security Threat Risk Assessment (STRA) in accordance with the **IMIT 6.11 STRA Standard** to identify and manage critical and high security risks. See the **MDSS 2.2** for more details;

b) Ensure that enrolled mobile devices and their operating systems are securely configured and securely deployed as per BC Government policies and standards; and,

c) Configure and enforce encryption for all storage on the enrolled mobile devices, including any removable storage (see **MDSS 2.3**). The cryptographic controls must meet the minimum requirements as per the **IMIT 6.10 Cryptographic Standards**.

5.1.5. Ministries in collaboration with the OCIO MUST ensure that:

a) Mobile devices are approved by the OCIO (see **MDSS 2.4** for more details);

b) Mobile devices capable of connecting to a data network or storing data are managed and enrolled into a Government of BC approved MDM system (except in limited and specific circumstances outlined in Section 5.4.3 of this standard) before they are used to process, access, or store personal or otherwise confidential Government of BC information;

c) Any mobile device that has not been in contact with a Government approved MDM system for 60 days is removed from the MDM system and its access to government networked resources blocked;

d) A mobile device is replaced as soon as possible with an OCIO approved device if its OS cannot be updated to the current release or prior release, or if there has been no patch or update for the OS in one year; and,

e) All mobile devices are tracked and inventoried regardless of their enrolment in the MDM system. See **MDSS 2.5** for mobile device inventory information details.

5.1.6. Ministries MUST:

a) Identify and report lost or stolen mobile devices immediately, regardless of value, in accordance with **Core Policy and Procedures Manual (CPPM) Chapter L: Loss Reporting** and the **Information Incident Management Policy**;

b) Ensure that data on mobile devices is protected and classified as per the **IMIT 6.18 Information Security Classification Standard** and guidelines;

c) Work with their Ministry Privacy Officer(s) and Ministry Information Security Officer(s) to ensure that personal information within mobile devices is protected with reasonable security measures as per the **Freedom of Information and Protection of Privacy Act (FOIPPA).** PIAs are required, as per *FOIPPA* and the **Privacy Management & Accountability Policy**; and,

d) Review reports of lost/stolen mobile devices regularly to identify enhancements to security awareness programs and compliance programs.

5.1.7. When contractor services are used, Ministries MUST ensure:

a) Contractor owned mobile devices that are to be connected to a BC Government provided network have a supplier supported operating system that can be updated to the latest release and are enrolled in the MDM system as a contractor;

b) Contractors follow the Contractor BYOD Terms of Use and only store BC Government data within the Apps managed through the MDM system;

c) Confidential government data (personal and sensitive) is removed from the contractor's device upon contract termination;

d) Service providers, including contractors that are using government-issued mobile devices comply with BC Government policies and standards, non-disclosure agreements and contracts governing their provisioning and operation; and,

e) Reputable anti-malware is installed on contractor-owned Android based devices used for conducting internal BC Government business. See **MDSS 2.6** for more details.

## 5.2. Design, Development, Testing & Management:

5.2.1. The OCIO MDM Service Owner MUST:

a) Ensure the Government of BC approved MDM system platform has the required capabilities for secure management of mobile devices. See **MDSS 3.1** for details.

b) Monitor and log:

i. Attempts to tamper with the mobile device operating system and block them; and,

ii. Vulnerable systems, i.e. mobile devices with operating systems (OS) that are no longer supported by the vendor for identification and removal from the MDM system.

c) Ensure that the data in transit and at rest is encrypted and the cryptographic controls meet the minimum requirements as per the **IMIT 6.10 Cryptographic Standards**;

d) Develop, document, maintain, implement, and make available and publish operating procedures and responsibilities that maintain the security of mobile devices;

e) Ensure changes to mobile device configuration and the MDM system follow the organization's change management process, including changes being tested and authorized before implementation in production systems; and,

f) Consider independent security assurances for the MDM system to meet any required legal or regulatory requirements it may have (e.g. PCI) and BC Government policies & standards (e.g. **IMIT 5.10 Critical Systems Standard**).

5.2.2. Ministries developing Apps for mobile devices MUST obtain digital signatures for their Apps. See **MDSS 3.2** for more details.

## 5.3. Implementation, Operations & Disposition:

5.3.1. The OCIO MDM Service Owner MUST:

a) Develop and maintain current, accurate and available documentation for mobility management that is necessary for ongoing support/operations (e.g. incident management);

b) Decommission enrolled mobile devices that are no longer on the OCIO's pre-approved list within 2 months after ministries have been notified;

c) Ensure data on mobile devices slated to be redeployed are securely wiped clean prior to being issued to new users; and,

d) Remove any mobile device that has not been in contact with a Government approved MDM system for 60 days from the MDM Service and its access to government networked resources blocked.

5.3.2. Ministries MUST ensure:

a) Mobile devices capable of connecting to a data network or storing data are managed and enrolled into a Government of BC approved MDM system (except in limited and

specific circumstances as outlined in Section 5.4.3 of this standard) before they are used to process, access, or store personal or otherwise confidential Government of BC information;

b) A mobile device is replaced as soon as possible with an OCIO approved device if its OS cannot be updated to the current release or prior release, or if there has been no patch or update for the OS for a year;

c) Mobile devices and any associated removable storage devices are disposed of in accordance with the **IMIT 6.06 IT Asset Disposal Standard**; and,

d) Government information stored on mobile devices is retained in compliance with the Information Management Act before disposal or reassignment of the devices. See **MDSS 4.1** for details.

5.3.3. Mobile devices that serve as workstations MUST:

a) Be installed with a firewall or network filtering technologies to protect them against network-based attacks when they are connected to non-government networks;

b) Where remote access is enabled, the devices must be configured to prevent their use as a conduit between non-government networks and government networks (e.g. VPN split-tunneling must be disabled);

c) For multi-user devices, unauthorized access by a user to another user's information stored on the device must also be prevented; and,

d) User authentication and remote access user authentication on these devices are in accordance with Government authentication policies/standards.

## 5.4. Limited and Specific Circumstances:

5.4.1. Based on balancing business needs with risks, modifications to the default MDM configuration profile may be requested by Ministries to the OCIO MDM Service Owner - this includes adjusting access controls, such as password and screen lock settings, to meet business requirements, providing adequate controls exist to protect confidential (personal and or sensitive) government information.

5.4.2. The OCIO MDM Service Owner MUST be consulted to use an unapproved mobile device. See **MDSS 5.1** for more details on the use of unapproved mobile devices.

5.4.3. Specific circumstances that do not require an IMIT exemption are as follows:

a) Kiosk or public display devices – see **MDSS 5.2** for more information; and,

b) Mobile devices that are used solely as a GPS or emergency phones – see **MDSS 5.3** for more guidance.

## 5.5. Training and Awareness:

5.5.1. Ministries, in collaboration with Ministry of Finance and OCIO, MUST provide employees with security, privacy, information management and records management awareness/training. See **MDSS 6.1** and **6.2** for more guidance.

## 6. SUPPORTING DOCUMENTS

- IMIT 5.10 Critical Systems Standard
- IMIT 6.06 IT Asset Disposal Process
- IMIT 6.10 Cryptographic Standards
- IMIT 6.11 STRA standard
- IMIT 6.19 Information Security Standard
- IMIT 6.24 Access Control Security Standard
- Core Policy and Procedures Manual (CPPM) Chapter L: Loss Reporting
- Information Incident Management Policy
- Privacy Management & Accountability Policy
- Information Security Classification Guidelines
- MySC KB0031397 article: Security Information for Corporate Mobile Devices on OCIO My Service Centre.

## 7. DEFINITIONS/GLOSSARY

**Anti-malware:** An umbrella term for software that detects and blocks unwanted input to the mobile device or computer, including viruses, Trojans, spyware, adware, and spam.
**Enterprise Mobility Management system:** A collective set of tools, technologies, processes, and policies used to manage and maintain the use of mobile devices.
**OCIO:** The organization in government that leads strategy, policy and standards for telecommunications, information technology, IT security and the management of the IM/IT investment portfolio for the Province.
**OS:** The master control program in a computer or mobile device.
**Service Owner:** The Single Point of Contact who is accountable for all aspects of a service throughout the service life cycle.

## 8. REVISION HISTORY

| Version | Revision Date | Author | Description of Revision |
|---|---|---|---|
| 1.1 | 2017-03-31 | Bashar Dari | Minor updates |
| 2.0 | 2018-01-10 | Marceline Cook | Rewrite, addition of contractor language, 90-day removal & more. Includes updates from ASRB review. |
| 3.0 | 2021-11-05 | Daniel Surdu & Sharina 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 |
| 3.0 | 2022-01-17 | Sharina Gopaldas Johnston | Correction of typos |

## 9. CONTACTS

For questions or comments regarding this standard, please contact:

ISB Branch, OCIO
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca