Document Version: 1.10
Effective Date: November 2021
Reviewed Date: November 2022

MOBILE DEVICE SECURITY SUPPLEMENTAL

1. INTRODUCTION

This document is established to clarify/supplement the security controls stated in the Mobile Device Security (MDS) Standard for use of mobile devices and secure mobile device management to protect confidential (personal or sensitive) government information. The baseline security controls listed in the standard and this document support the Defensible Security principles for the protection of government confidential information and MUST be applied for the management of information and mobile devices used for government work. Privacy Impact Assessments (PIA) and Security Threat and Risk Assessments (STRA) may identify additional mobile device security requirements to those outlined in this document and the standard.

2. MOBILE DEVICE PLANNING, ACQUISITION & REQUIREMENTS

2.1. Device Services MUST ensure the mobile devices and their operating systems are compliant with the Information Security Policy (ISP) – Sections 2.1 and 7, and the IMIT Standards 6.10, 6.24 and 6.28.

2.2. A Security Threat Risk Assessment (STRA) MUST be completed for:

a) Each new mobile device that is to be approved, if that device differs in a way that could present a new or increased risk by its type, make or model.
b) Each approved mobile device's major operating system release that introduces significant change in function/feature.
c) Each Mobile Device Management (MDM) system itself and its upgrades.

2.3. Encryption for removable storage (for example, SD cards, USB) used with enrolled mobile devices also MUST be enforced.

2.4. Approved mobile devices have been assessed by the Office of the Chief Information Officer (OCIO) MDM Service Owner to meet or exceed the requirements of the published MDS standard to store confidential government information. Approved mobile devices also have a supplier supported operating system that can be updated to the latest release. Ministries wishing to use an unapproved mobile device MUST do the following before acquiring it:

a) Consult with the OCIO MDM Service Owner on its use for government business.

b) Complete a STRA for the mobile device to ensure that its use does not pose an unacceptable security risk or conflict with OCIO strategic objectives.

c) Apply for an IMIT exemption to the MDS standard through the OCIO to use an unapproved mobile device when it can be demonstrated that its use does not pose an unacceptable security risk or conflict with OCIO strategic objectives.

2.5. Both Ministries and the OCIO MDM Service Owner MUST collaborate to ensure that all mobile devices are tracked and inventoried regardless of their enrolment in the MDM system. Ministries MUST notify the OCIO MDM Service Owner of changes made to the mobile devices issued by the OCIO that are in their custody, for instance, reassignments, disposal, operating system change (for example, from Windows to Linux) or function (for example, from kiosk to user, or from emergency phone to smartphone). At minimum, the information captured in the inventory for mobile devices should contain the following information:

- Assignee.
- Manufacturer.
- Device make and model.
- Operating system and version number.

2.6. Any up-to-date anti-malware available from the reputable established anti-malware developers for Android based devices (for example, Trend, McAfee, Norton, Kaspersky) downloaded from Google Play app store will be acceptable.

3. DESIGN, DEVELOPMENT, TESTING & MANAGEMENT

3.1. The BC Government approved MDM system platform at minimum, MUST be able to:

a) Provide asset management capabilities to ministries for enrolled mobile devices. The minimum information that the MDM system platform MUST capture are:

- Unique identity of the user to whom the device is assigned.
- Manufacturer.
- Device make and model.
- Operating system version.
- Apps/applications/software installed.
- Device status.
- Last contact time.
- Enrollment.

b) Enable application of corporate and ministry level policies.

c) Deny the enrolment of unapproved mobile devices, including those that are jail-broken or rooted.

d) Configure and enforce access controls such as screen locks and PIN/passwords on all enrolled mobile devices.

e) Allow for remote management of all enrolled mobile devices, for example, locking it, PIN/password reset/change and wiping of the device.

f) Push out Operating System (OS) and pre-installed standard apps/applications/software patch updates to all enrolled mobile devices.

g) Install and update anti-malware app on all enrolled mobile devices where it adds value (for example, Android, Windows, Macs). It is not necessary for mobile devices where the device manufacturer has already taken steps to protect the device from malware (for example, iOS) - see Supporting Documents Section.

h) Support multi-factor authentication.

i) Maintain and enforce allowlist and denylist of apps/applications/software and block the installation of denylisted apps/applications/software.

j) Support/enable device restrictions to limit device functionality.

k) Push out compliance policies on the following:

1. Device and OS configuration settings that are compliant with BC government policies and standards.
2. Password requirements that are compliant with the **IMIT 6.24 Access Control Security Standard*.**
3. Screen-lock enrolled mobile devices after an idle duration that doesn't exceed 15 minutes.
4. Removal of denylisted apps/applications/software from the enrolled mobile devices.

***** If the password authentication on mobile devices cannot comply with the **IMIT 6.24 Access Control-Complex Password Standard** for government, the minimum password of at least 6 characters MUST be leveraged on mobile devices along with external two-factor authentication or approved biometrics.

Biometrics for mobile devices are:

Biometric Technology	**Apple**	**Samsung Android**
Fingerprint scanners	Approved	Approved

Biometric Technology	Apple	Samsung Android
Facial recognition	Approved	Not approved

3.2. Ministries developing Apps for mobile devices MUST work with CITZ Data Platforms and Data Division DevOps and Cloud Services - Platform Services team to obtain digital signatures for their Apps. Refer to the BC Government Team Mobile Services site for more information.

4. IMPLEMENTATION, OPERATIONS & DISPOSITION

4.1. Ministries MUST ensure all government information stored on mobile devices (and removable storage media used with the devices) are:

a) Backed up to protected office recordkeeping systems prior to disposal.

b) Retained according to their approved information schedule.

4.2. Ministries MUST dispose of mobile devices (or removable storage media) following the **IMIT 6.06 IT Asset Disposal Process.**

5. LIMITED AND SPECIFIC CIRCUMSTANCES

5.1. Unapproved mobile devices may be allowed for temporary use when:

a) There are technical limitations (for example, there is no MDM software agent available, or the MDM software agent cannot be installed on the mobile device due to its lack of technical capability). Such devices MUST be with replaced with an approved mobile device as soon as possible.

b) The mobile devices that have the technical capability to access data networks (e.g. Wi-Fi) and store information but are not configured with a cellular data plan.

5.2. Mobile devices that do not store or have any access to confidential (personal or sensitive) government information may be used as kiosk or public display devices. No IM/IT exemption is required for these devices.

5.3. No IM/IT exemption is required when a mobile device is used solely as GPS or emergency phone and DOES NOT:

- Have cellular data network access plans configured.
- Have Wi-Fi data network access configured.
- Store and have no access to any confidential (personal and sensitive) information.

6. TRAINING AND AWARENESS

6.1. The awareness/training to be provided to employees who use mobile devices MUST ensure their:

a) Familiarity with the operation and use of protection technologies.
b) Familiarity with the **Information Incident Management Policy** including the requirement for BC Government to delete all data (including personal data) from a lost or stolen device.
c) Awareness of the additional risks and responsibilities inherent in mobile computing and when using mobile devices.
d) Awareness to not leave mobile devices unsecured and unattended.

6.2. The **Appropriate Use Policy** provides guidance on the use of IM/IT resources and links to the **Mobile Device Guidelines** (MDG). The MDG provides user-centric detailed guidance on how to protect their government-issued mobile devices and the information stored on them.

7. SUPPORTING DOCUMENTS

- IMIT 6.06 IT Asset Disposal Process
- IMIT 6.24 Access Control Security Standard
- Information Incident Management Policy
- Appropriate Use Policy
- Mobile Device Guidelines
- Why AV doesn't provide the same level of protection on iOS devices: https://support.apple.com/en-ca/guide/security/sec35dd877d0/1/web/1

8. DEFINITIONS/GLOSSARY

The following key words in this document are to be interpreted as described in RFC 2119 (see https://tools.ietf.org/html/rfc2119):

- MAY;
- MUST;
- MUST NOT;
- OPTIONAL;
- RECOMMENDED;
- REQUIRED;
- SHALL NOT;
- SHALL;
- SHOULD; and
- SHOULD NOT

9. REVISION HISTORY

Version	Revision Date	Author	Description
1.0	November 2021	Sharina Gopaldas Johnston	New release.
1.1	November 2022	Sharina 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.

10. CONTACTS

For questions or comments regarding this standard, please contact:
Information Security Branch, Office of the Chief Information Officer
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca