MOBILE DEVICE SECURITY STANDARD FOR INFORMATION PROTECTION

Information Security Branch
Office of the CIO ● Province of BC
People ● *Collaboration* ● *Innovation*

Document Version 1.1
Published: March 31, 2017

Replaces: None

Introduction

This document contains standards for the protection of confidential (personal and sensitive) information on mobile devices. These standards are developed in collaboration with ministries, endorsed by the Architecture and Standards Review Board and approved by the Government Chief Information Officer.

Applicability

These standards apply to mobile devices that are used to access, process or store BC government information. This standard applies to mobile devices owned by the BC government. These standards will establish the baseline security controls for secure mobile device use and protection of confidential (personal and sensitive) information.

Privacy Impact Assessments (PIA) and Security Threat and Risk Assessments (STRA) may identify additional mobile device security requirements.

Compliance Schedule

A compliance schedule will be developed in cooperation with ministries, endorsed by the Architecture and Standards Review Board and approved by the Government Chief Information Officer.

For existing mobile devices:
Existing mobile devices must be brought into compliance unless it can be demonstrated that the devices cannot store confidential (personal and sensitive) information.

For new mobile devices:
Only devices that meet or exceed the published standard can be procured.
Where a new mobile device cannot reasonably be made compliant with this standard, but does not pose an unacceptable security risk or conflict with OCIO strategic objectives, then an exemption may be applied for through the Office of the Chief Information Officer (OCIO).

It is expected that mobile devices that are capable of storing confidential (personal and sensitive) information will have adequate security controls enforced by an Enterprise Mobility Management (EMM) system (i.e. Mobile Device Management Service (MDMS)).

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.

Applications: Software programs on a computer or mobile device. In the case of mobile devices, these would include mandatory applications needed by MDMS.

ASRB: Architecture & Standards Review Board, establishes, owns and manages the content of the Enterprise Architecture Strategy. ASRB reviews IT standards and advises GCIO to approve them or not.

AUP: Appropriate Use Policy, stipulates constraints and practices that a user must agree to for access to BC Government systems.

Contractor: See Service Provider.

EMM: Enterprise Mobility Management, a collective set of tools, technologies, processes and policies used to manage and maintain the use of mobile devices.

GCIO: Government Chief Information Officer, in charge of information security strategy.

MDM: Mobile Device Management, see EMM.

MDMS: Mobile Device Management Service, BC Government's service implementation of EMM.

MISO: Ministry Information Security Officer: The single point of contact for information security issues and related concerns in the Ministry. For more information about MISOs role, refer to Link. For a list of all MISOs, refer to this Link.

Mobile Device: A computing device primarily designed for mobile use, such as:

- Smartphones, Internet enabled mobiles
- OCIO-Defined Tablets

Laptops are not included in this definition.

MPO: Ministry Privacy Officer: The single point of contact for privacy issues and related concerns in the Ministry. For more information about MPOs role, refer to this link. For a list of all MPOs, refer to MPO Directory.

OCIO: Office of the Chief Information Officer (OCIO) leads strategy, policy and standards for telecommunications, information technology, IT security and the management of the IM/IT investment portfolio for the Province.

OS: Operating System, the master control program in a computer or mobile device.

PIA: Privacy Impact Assessment, an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Service Owner: the Single Point of Contact who is accountable for all aspects of a service throughout the service life cycle.

Service Provider: a person or an organization retained under contract to perform services for the Government of British Columbia.

STRA: Security Threat Risk Assessment, a tool for understanding the various threats to IT systems, determining the level of risk these systems are exposed to, and recommending the appropriate level of protection.

Standard/Controls:

Mobile Device Planning, Acquisition & Requirements

1. MDMS Service Owner must identify security requirements for new mobile devices or operating systems, and for enhancements to existing systems, as per the Information Security Policy (Section 2.2). OCIO Device Services is the MDMS Service Owner.

2. The OCIO must complete a Security Threat Risk Assessment (STRA) for:

    - Each class of mobile devices and
    - Each mobile device's major operating system release and
    - Each mobile device's minor release when needed and
    - MDMS.

    OCIO must ensure that critical and high security risks are managed. The STRA must include documented approvals of mitigation plans, residual risks and documentation of their acceptance.

3. Ministries, in collaboration with the OCIO, must maintain an inventory of mobile devices including but not limited to key information such as assignee, manufacturer, model, and operating system.

4. Ministries, in collaboration with the OCIO, must ensure mobile devices are enrolled in MDMS and have the MDMS agent installed and active on the mobile devices at all times.

5. Mobile devices that do not have the technical capabilities to connect to data networks (e.g. Wi-Fi, cellular data) do not require the installation of the MDMS agent, but must still be tracked by Ministries and maintained in the inventory of mobile devices.

6. Mobile devices that have the technical capability to access data networks (e.g. Wi-Fi, cellular data) and store information, even if not configured with a cellular data plan, must have the MDMS agent installed and active on the mobile device.

7. If an existing mobile device has technical limitations (e.g. there is no MDMS software agent available or the MDMS software agent cannot be installed on the mobile device due to lack of technical capability), such mobile devices may be used temporarily until the device is replaced with a compliant one as soon as reasonably possible.

8. New mobile devices must be compliant and have the necessary technical capabilities to support the installation of the MDMS software agent.

9. Ministries must identify and report lost and stolen mobile devices immediately, according to Core Policy and Procedures Manual Procedure L (Loss Reporting) and Information Incident Management Process.

10. Ministries must ensure that data on mobile devices is classified and protected as per the Information Security Classification Framework and Information Security Policy.

11. Ministries must work with their Ministry Privacy Officer(s) (MPO) and Ministry Information Security Officer(s) (MISO) 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 Privacy Management & Accountability Policy.

12. Service Providers and Contractors using Government-supplied mobile devices must comply with BC government policies and standards, non-disclosure agreements and contracts governing their service provisioning and operation. Upon termination, confidential (personal and sensitive) data must be removed.

13. MDMS Service Owner must ensure that mobile devices and their operating systems are securely configured and securely deployed as per BC government policies and standards.

14. Ministries must retain government information in accordance with an approved information schedule in accordance with the Information Management Act. Government information must not be disposed of if no information schedule applies.

Design, Development & Testing

15. MDMS Service Owner must ensure that cryptographic controls meet the minimum requirements for data in transit and at rest (e.g. AES 256-bit), as per the Cryptographic Standards for Information Protection.

16. Password authentication on mobile devices must comply with the 'Access Control-Complex Password Standard for government' section of the Information Security Policy or leverage a password of at least 6 characters or an approved authentication mechanism that is as good or stronger (e.g. biometrics).

17. MDMS Service Owner must develop, document, maintain and implement operating procedures and responsibilities that maintain the security of mobile devices.

18. Mobile devices must have a screen-lock password enabled. Settings for idle duration before automatic screen-lock must not exceed 15 minutes.

19. MDMS Service Owner must ensure changes to mobile device configuration and the Mobile Device Management Service (MDMS) follow the organization's Change Management process, including changes being tested and authorized before implementation in production systems.

20. MDMS Service Owner must consider independent security assurances for mobile device management systems as per Acts, regulations (e.g. PCI) and BC government policies & Standards (e.g. Critical Systems Standard).

Implementation, Operations & Disposition

21. Ministries, in collaboration with OCIO, must ensure that mobile devices, regardless if they have access to email or not, are managed under MDMS except if they fall under 'Limited and Specific Circumstances'.

22. MDMS Service Owner must develop and maintain as current, accurate and available, documentation for mobility management that is necessary for ongoing support/operations (e.g. incident management).

23. Employees accessing data via government-supplied mobile devices must comply with BC government policies and standards including the AUP. Employees must store electronic records that relate to government business on Protected Government Systems.

24. Employees must have supervisor permission before installing apps or software on their government-supplied mobile devices regardless if they are for personal or business use. See the AUP as well as the Application and Software Guide for more information.

25. MDMS Service Owner must ensure the availability of recommended anti-malware software for government-supplied mobile devices. Ministries must ensure that their Mobile Devices have installed and up-to-date anti-malware software, as available and provided.

26. Employees must apply mobile device patches and system updates, once they have been approved by OCIO, on a regular and timely basis commensurate with the criticality and risks of the sensitivity of the information on the mobile device.

27. Ministries must ensure that mobile devices and any associated electronic storage devices are disposed of according to the IT Asset Disposal Standard and Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia. Mobile devices slated to be redeployed must be wiped clean of data, prior to being issued to a new user.

28. If the mobile device is two Operating Systems (OS) versions/releases behind, Ministries must update to the latest version. If a device cannot be updated to the latest version of the OS, it should be replaced by a new mobile device. If a patch or update hasn't been released for the OS in two years, the mobile device should be replaced.

29. Employees must immediately report information incidents involving the actual or suspected loss of information and/or information incidents regardless of value.

Mobile Device Management

30. Ministries must work with OCIO to ensure mobile devices have the MDMS software agent installed and are configured to connect to a Government approved Mobile Device Management System (MDMS) to:
    - enable application of corporate and ministry level policies
    - provide asset management capabilities to ministries
    - detect and block system modifications resulting in jail-broken or rooted devices

- provide ministries with a clear view of applications on devices
- provide ministries with access to anti-malware for mobile as applicable
- detect and block non-approved devices including those that are jail-broken or rooted
- identify malicious apps and vulnerable systems
- configure and enforce encryption for all storage on the mobile devices, including any removable storage (e.g. SD cards, USB, and so on.)
- configure and enforce access controls such as screen lock and PIN/passwords.
- allow for remote management of device such as locking it, changing password and wiping of device.
- providing reporting capability on device status which includes things like last contact time and enrollment state.

31. In certain limited and specific circumstances, and based on balancing business needs with risks, modifications to the default configuration profile may be considered in order to address certain specific business requirements. This includes adjusting access controls, such as password and screen lock settings, to meet the business requirements, as long as adequate controls exist to protect confidential (personal and sensitive) information. These circumstances include:

    - **Kiosk or public display devices**, that do not store or have any access to confidential (personal and sensitive) information

    - Mobile devices that are used **solely as a GPS** or **emergency phones** and:
        1. Do not have cellular data network access plans configured
        2. Do not have Wi-Fi data network access configured
        3. Do not store and have no access to any confidential (personal and sensitive) information

32. Mobile devices are issued by Government when there is a business reason for doing so, in accordance with corporate standards. Users must take reasonable precautions to safeguard these mobile devices and the Government information residing on them – for example, not leaving mobile devices unsecured and unattended.

Training and Awareness

33. Ministries, in collaboration with Ministry of Finance and OCIO, must provide Employees with security, privacy, information management and records management awareness/training to ensure that they are:
    - Aware of their responsibility to immediately report Information incidents involving the actual or suspected loss of information and/or information technology security incidents including loss/theft of mobile device, regardless of value,
    - Familiar with the operation and use of protection technologies,
    - Familiar with the Information Incident Management Process including the requirement for BC Government to delete all data from a lost or stolen device,
    - Aware of the additional risks and responsibilities inherent in mobile computing and when using mobile devices.