Office of the Chief Information Officer

MOBILE DEVICE SECURITY STANDARD FOR INFORMATION PROTECTION

Information Security Branch
Office of the Chief Information Officer | Province of BC

Document Version 2.0
Published: November 22, 2017

Replaces: Version 1

Document History

Date	Author	Version	Change
March 31st 2017	Bashar Dari	1.1	Minor updates
November 22th 2017 / January 10th 2018	Marceline Cook	2.0	Rewrite, addition of contractor language, 90 day removal & more. Includes updates from ASRB review.

Introduction

These standards apply to mobile devices that are used to access, process or store BC government information. This establishes the baseline security controls for secure mobile device use and protection of confidential (personal and or sensitive) information. Privacy Impact Assessments (PIA) and Security Threat and Risk Assessments (STRA) may identify additional mobile device security requirements to those outlined in this standard.

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:
New Devices must meet or exceed the published standard .
An exemption to the standard may be applied for through the Office of the Chief Information Officer (OCIO) where it can be demonstrated that a new mobile device cannot reasonably be made compliant, but does not pose an unacceptable security risk or conflict with OCIO strategic objectives.

Devices acquired must have a supplier supported operating system that can be updated to the latest release.

Mobile devices that are capable of storing confidential (personal and sensitive) information must be able to have adequate security controls enforced by a BC Government 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.

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

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 Role of MISO. For a list of all MISOs, refer to this MISO List.

Mobile Device: Portable and self-contained electronic devices that can connect to the government network. This includes but is not limited to tablets, smartphones, and cellphones. Laptops are not included in this standard.

MPO: Ministry Privacy Officer: The single point of contact for privacy issues and related concerns in the Ministry. For more information about the MPO role refer to the Privacy Management and Accountability Policy. For a list of all MPOs refer to the 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. The 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 OCIO Device Services is the MDMS Service Owner.

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

    - Each mobile device; if that device differs in a way that could present a new or increased risk
    - Each mobile device's major operating system release and
    - Each mobile device's minor release as determined by the OCIO
    - Each MDMS

3. The 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. Minor releases are assessed by the OCIO on a case-by-case basis and may generate the need for an STRA.

4. Ministries, in collaboration with the OCIO, must maintain an inventory of mobile devices including but not limited to:

    - Assignee
    - Manufacturer
    - Device make & model
    - Operating system & version number

5. Ministries in collaboration with the OCIO must ensure that mobile devices capable of connecting to a data network are managed by an approved MDMS, except in limited and specific circumstances as outlined in this standard.

6. Ministries must, in collaboration with the OCIO actively review and remove device access to government networks through the MDMS if the device has not been in contact with the MDMS for 60 days.

7. Ministries must identify and report lost and stolen mobile devices immediately, regardless of value, according to the Core Policy and Procedures Manual Procedure (Loss Reporting) and the Information Incident Management Process.

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

9. Ministries must work with their MPO(s) and MISO(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.

10. Service Providers including Contractors that are using 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.

11. Contractor owned mobile devices that are to be connected to a BC Government provided network must be enrolled in the MDMS as a contractor and follow the Contractor BYOD Terms of Use. Contactors must only store BC Government data within the container Apps managed through the MDMS.

12. The 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.

13. Ministries must retain government information according to an approved information schedule in compliance with the *Information Management Act*. If there is no applicable information schedule, government information must not be disposed.

Design, Development & Testing

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

15. 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, external two factor authentication or approved biometrics.

    Approved biometrics for mobile devices are:

    - Fingerprint scanners
    - iPhone X Facial recognition

16. The MDMS Service Owner must ensure a screen-lock password is enabled. Settings for idle duration before automatic screen-lock must not exceed 15 minutes.

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

18. The 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.

19. The MDMS Service Owner must consider independent security assurances for mobile device management systems to meet any required legal or regulatiory requirements they may have (e.g. PCI) and BC government policies & standards. (i.e. Critical Systems Standard).

20. Ministries developing Apps for mobile devices must consult the CITZ Innovation Hub when developing and testing Apps.This is to ensure Apps are created and tested to BC Government standards.

Implementation, Operations & Disposition

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

22. 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.

23. Before installing an App from a public App store, or side loading Apps (manually installing an App to a device without going through an official App store) onto a BC Government supplied device that is intended to process, access or store BC Government data employees must have supervisor permission and have completed a mobile STRA and PIA. See the AUP as well as the Application and Software Guide for more information.

24. If using software from a BC Government supplied App Store, supervisor permission is not required for app installation. However, if the use case for the app is different from that of the approved software in the BC Government supplied App Store, a new STRA and PIA must be completed.

25. Supervisor permission and an STRA/PIA are not required to download apps from Apple's App Store, Google Play or Blackberry World that are not going to be used to process, access or store BC Government data, e.g. flashlight app.

26. The 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.

27. Android based devices used for conducting internal BC Government business, including those used by contractors, must have reputable anti-malware installed.

28. Employees must apply mobile OS patches when released unless specified otherwise by the OCIO. System updates must be applied once they have been approved by OCIO.

29. 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.

30. Mobile devices can only be one major (e.g. 7.x vs 8.0) OS behind the current release. If a device cannot be updated to the current release it should be replaced by a new mobile device as soon as reasonably possible. If a patch or update hasn't been released for the OS in one year, the mobile device must be replaced as soon as reasonably possible with a compliant device.

Mobile Device Management

31. 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
    - 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
    - Provide reporting capability on device status, including last contact time and enrollment state
    - OCIO will through periodic scans remove devices that are not up to the required OS level after warnings have been provided to clients

Limited and Specific Circumstances

32. In certain limited and specific circumstances, and based on balancing business needs with risks, modifications to the default MDMS configuration profile may be requested. This includes adjusting access controls, such as password and screen lock settings to meet business requirements as long as adequate controls exist to protect confidential (personal and or sensitive) information.

A request to use a non-compliant device should go through the MDMS service provider. For example:

- Mobile devices that have 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) may be used temporarily until the device is replaced as soon as reasonably possible with a compliant device
- An exemption is required for mobile devices that are not connected to the MDMS but have the technical capability to access data networks (e.g. Wi-Fi) and can store information, even if not configured with a cellular data plan

Some specific circumstances that are not required to go through the security exemption process include:

- Kiosk or public display devices, that do not store or have any access to confidential (personal and sensitive) information. These devices do not need to go through the security exemption process
- Mobile devices that are used solely as a GPS or emergency phones and:
    i. Do not have cellular data network access plans configured
    ii. Do not have Wi-Fi data network access configured
    iii. Do not store and have no access to any confidential (personal and sensitive) information

Regardless of enrolment in MDMS, all devices must still be tracked by Ministries and maintained in an inventory of mobile devices.

Training and Awareness

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

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

35. 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:

    - 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
    - Aware they are not to leave mobile devices unsecured and unattended