Ontario

UNCLASSIFIED

Government of Ontario IT Standard (GO-ITS)

GO-ITS Number 25.10

Security Requirements for Mobile Devices

Version 1.4

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

© Queen's Printer for Ontario, 2015

Last Review Date: 2015-03-18

Copyright & Disclaimer

For third party users, including government contractors and entities seeking to provide products or services to the Government of Ontario, the Government of Ontario does not represent or warrant to you the accuracy, suitability or completeness of the content of this document.

© 2015 Government of Ontario. All rights reserved.

Other product or brand names are trademarks or registered trademarks of their respective holders. This document contains proprietary information of Government of Ontario, disclosure or reproduction is prohibited without the prior express written permission from Government of Ontario.

Template Info

Template Name	Template #	Template Version No.	Template Author	Template Completion Date
GO-ITS Template	09.03.26	2.0	Design: PMCoE Boilerplate: CAB/OCCS	2009-03-26

Document History

Date	Summary
2006-01-18	**Endorsed:** IT Standards Council (ITSC) endorsement
2006-02-28	**Approved:** Architecture Review Board (ARB) approval
2006-03-15	**Revised:** Changed the section on Safeguards for Integrated Handhelds/PDAs, as follows: • Changed requirement for alphanumeric password to a recommendation; i.e., now reads "should include at least one number and one letter" instead of "must include…" • Changed requirement for periodic change of passwords (every ninety days or less) to a recommendation • Changed requirement for 20 minute inactivity timeout to a recommendation
2006-04-19	• Changes noted above (i.e. from March 15/06) endorsed by the ITSC • Published as GO-ITS 25.10, approved version number 1.1
2009-02-09	**Revised:** • Updated contact information to reflect organizational changes • Added details based on feedback received from end users of standard and audit input • Changes to language and tone throughout • Adjusted roles and responsibilities • Revised discussion of sensitive information • Enhanced discussion regarding RIM BlackBerry use. Draft version number set to 1.2
2009 (March-April)	• Draft endorsed by ITSC (March 18/2009 minutes of ITSC meeting), however, publication deferred pending report back to ARB on action items (April 23/2009 ARB minutes)
2011-02-07	**Revised:** • Adjusted cryptography guidance • Adjusted removable media guidance as per ITSC input • Updated BlackBerry guidance in light of new information regarding content protection performance • Updated password guidance wording re: GO-ITS 25.15 *Security Requirements for Password Management and Use* • Updated glossary, acronyms, and references • Format changed to new ITSC GO-ITS layout

2011-04-05	• Adjustments as per ITSC member feedback
2011-04-20	**Endorsed:** IT Standards Council endorsement
2011-04-27	• Adjustments as per ITSC action items
2011-05-04	**Approved:** Architecture Review Board approval
2011-05-13	• Final adjustment as per ITSC and ARB minutes. Approved version number set to 1.3
2015-01-19	• Minor change per ARB rationale (administrative updates, ISO/IEC alignment), draft document version number set to 1.4
2015-03-06	• Minor adjustment as per received ARB feedback
2015-03-18	Endorsed by Architecture Review Board (ARB)
2015-04-16	Approved by Information Technology Executive Leadership Council (ITELC)

Table of Contents

Foreword

Government of Ontario Information Technology Standards (GO-ITS) are the official publications on the guidelines, preferred practices, standards and technical reports adopted by the Ontario Public Service under the delegated authority of the Management Board of Cabinet (MBC). These publications support the responsibilities of the Treasury Board Secretariat (TBS) for coordinating standardization of Information & Information Technology (I&IT) in the Government of Ontario. Publications that set new or revised standards provide enterprise architecture guidance, policy guidance and administrative information for their implementation. In particular, GO-ITS describe where the application of a standard is mandatory and specify any qualifications governing the implementation of standards.

All GO-ITS 25 Standards are based on the work of recognized global authorities in information and operational security, both in government and industry.

1. Introduction

1.1. Background and Purpose

This document describes security requirements for the use of mobile devices and technology within the Government of Ontario. It is intended to ensure that the use of mobile devices will not result in undue or unmitigated risk that jeopardizes the electronic delivery of Government services, or related information assets.

The primary audience for this document includes application developers, implementers and program managers. It is intended to directly influence the design, development, and deployment of applications operated on behalf of the Government of Ontario.

The following statements support and are stated in accordance with the Management and Use of Information & Information Technology (I&IT) Directive, the Corporate Policy on Information and Information Technology (I&IT), and ISPC policy:

- Ministries and agencies **must** be assured that the use of mobile devices for business purposes does not place sensitive information at risk – this assurance is expressed in terms of accountability, confidentiality, integrity, availability, reliability and the opportunity for audit;
- Mobile device implementations **must** offer a degree of security and assurance that compensates for the loss of some traditional safeguards (such as managed enterprise network perimeters and physical protective measures in office locations);
- Users are individually responsible for the ongoing protection of their mobile device(s) and the Government information that is stored on or accessed via such mobile device(s); and
- Government mobile devices are subject to inspection to ensure appropriate use, the integrity of the device, and compliance with these security requirements.

1.2. Scope

1.2.1. In Scope

The GO-ITS 25.10 Security Requirements for Mobile Devices apply to:

- All ministries of the Government of Ontario, and all individuals or organizations using mobile devices for Government purposes;
- Mobile communications, computing and data storage devices used by the Government of Ontario (e.g., cellular phones, mobile devices with cellular data connectivity);
- Portable computers (e.g., notebook/laptop PCs, tablet PCs, netbook PCs, Personal Digital Assistants [PDAs]); and
- Removable media (e.g., USB storage devices, portable hard drives, flash memory cards, optical disc media).

For the purposes of this document all references to “information” refer to digital information and data. Any reference to mobile devices includes all of the above categories of devices.

Appendix A of this standard contains specific technical requirements for RIM BlackBerry mobile devices.

For security involving sensitive information[1], if it becomes known that sensitive information is deemed at serious risk then immediate remedial action **must** be taken to mitigate the risk by applying the tools, methods, procedures etc. as per the relevant GO-ITS security document.

The Strategy, Planning, and Enterprise Architecture Branch (SPEAB) of the I&IT Strategy and Cyber Security Division (SCS), or a successor division/branch, should be contacted if the requirements in this document require clarification or if it is not clear whether this standard applies to a given situation.

1.2.2. Out of Scope

This standard does not apply to:

- Radio communication devices for voice communications (e.g., traditional UHF/VHF dispatch systems, portable/handheld radio devices, Family Radio Service [FRS] / General Mobile Radio Service [GMRS] devices);
- RF (radio frequency) access devices (e.g., proximity cards, RF smart cards, other RF identification [RFID] devices); and
- Non-storage digital device components (e.g., a digital camera body with no card inserted).

1.3. Applicability Statements

1.3.1. Organization

Government of Ontario IT Standards and Enterprise Solutions and Services apply (i.e., are mandatory) for use by all ministries/clusters and to all former Schedule I and IV provincial government agencies under their present classification (Advisory, Regulatory, Adjudicative, Operational Service, Operational Enterprise, Trust or Crown Foundation) according to the current agency classification system.

Additionally, this applies to any other new or existing agencies designated by Management Board of Cabinet as being subject to such publications, i.e. the GO-ITS publications and enterprise solutions and services - and particularly applies to Advisory, Regulatory, and Adjudicative Agencies (see also procurement link, OPS paragraph). Further included is any agency which, under the terms of its Memorandum of Understanding with its responsible Minister, is required to satisfy the mandatory requirements set out in any of the Management Board of Cabinet Directives (*cf*. Operational Service, Operational Enterprise, Trust, or Crown Foundation Agencies).

As new GO-ITS standards are approved, they are deemed mandatory on a go-forward basis (go-forward basis means at the next available project development or procurement opportunity).

[1] Sensitive information as defined per Information Security and Privacy Classification (ISPC) policy (http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.18.14.34.52.PSU_res/$File/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf).

When implementing or adopting any Government of Ontario IT standards or IT standards updates, ministries and I&IT Cluster must follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management, risk mitigation, and control selection mechanisms are in place and employed.

For the purposes of this document, any reference to ministries or the Government includes applicable agencies.

1.4. Requirements Levels

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	This word, or the terms "REQUIRED" or "SHALL", means that the statement is an absolute requirement.
Should	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore the recommendation, but the full implications (e.g., business functionality, security, cost) must be understood and carefully weighed before.

1.5. Contact Information

1.5.1. Roles and Responsibilities

Accountable Role Definition
The individual ultimately accountable for the process of developing this standard. There must be exactly one accountable role identified. The accountable person also signs off as the initial approver of the proposed standard before it is submitted for formal approval to ITSC and ARB. (Note: in the OPS this role is at a CIO/Chief or other senior executive level, e.g. Head, Director or higher)

Accountable Role:
Title: Manager, Security Policy and Standards Unit
Ministry/Cluster: Ministry of Government and Consumer Services
Division: I&IT Strategy and Cyber Security Division
Section: Cyber Security Strategy, Risk Management & Architecture Branch
Job Title: Manager
Name: Alex Fanourgiakis
Phone: (647) 982-5216
Email: Alex.Fanourgiakis@ontario.ca

Responsible Role Definition
The organization responsible for the development of this standard. There may be more than one responsible organization identified if it is a partnership/joint effort. (Note: the responsible organization provides the resource(s) to develop the standard)

Responsible Organization:
Ministry/Cluster: Ministry of Government and Consumer Services
Division: Cyber Security Division
Branch: Cyber Security Strategy, Risk Management & Architecture Branch

Support Role Definition

The support role is the resource(s) to whom the responsibility for actually completing the work and developing the standard has been assigned. There may be more than one support role identified. If there is more than one support role identified, the following contact information must be provided for each of them. If there is more than one support role, the first role identified should be that of the editor – the resource responsible for coordinating the overall effort.

Support Role (Editor):

Ministry/Cluster: Ministry of Government and Consumer Services
Division: Cyber Security Division
Branch: Cyber Security Strategy, Risk Management & Architecture Branch
Job Title: Sr. Security Policy Advisor

Name: Tim Dafoe
Phone: (416) 327-1260
Email: tim.dafoe@ontario.ca

Consulted

Please indicate who was consulted as part of the development of this standard. Include individuals (by role and organization) and committees, councils and/or working groups. (Note: consulted means those whose opinions are sought, generally characterized by two-way communications such as workshops):

Organization Consulted (Ministry/Cluster)	Division	Branch	Date
ITS EES / Blackberry Operations	MGS	ITS	Q4 2009
CSB Security Design and Policy	MGS	CSB	Q4 2009

Committee/Working Group Consulted	Date
ARB	Dec. 10th 2014

Informed

Please indicate who was informed during the development of this standard. Include individuals (by role and organization) and committees, councils and/or working groups.(Note: informed means those who are kept up-to-date on progress, generally characterized by one-way communication such as presentations):

Organization Informed (Ministry/Cluster)	Division	Branch	Date

Committee/Working Group Informed	Date

1.6. Recommended Versioning and/or Change Management

Changes (i.e. all revisions, updates, versioning) to the standard require authorization from the "responsible" organization. Once a determination has been made by the responsible organization to proceed with changes, the Strategy, Planning, and Enterprise Architecture Branch, OCCS, will coordinate and provide assistance with respect to the approvals process. The approval process for changes to standards will be determined based on the degree and impact of the change. The degree and impact of changes fall into one of two categories:

***Minor changes** - requiring communication to stakeholders, ARB endorsement required. Changes are noted in the "Document History" section of the standard.*

***Major changes** - requiring a presentation to ARB and ITELC for endorsement.*

Below are guidelines for differentiating between minor and major changes:

Major:

- represents a major version change to one or more specifications
- impacts procurement
- requires configuration changes to current solutions
- impacts other standards
- responds to legislative, policy or procurement changes

Minor:

- represents incremental version changes to one or more specifications
- does not impact procurement (other than informational)
- does not require configuration changes to current solutions
- does not impact other standards
- is not related to legislative, policy, or procurement changes

1.7. Publication Details

All approved Government of Ontario IT Standards (GO-ITS) are published on the OPS Intranet. Please indicate with a checkmark below if this standard is also to be published on the public GO-ITS Internet site.

Standard to be published on both the OPS Intranet and the GO-ITS Internet web site (available to the public, vendors etc.)	☑

1.8. Compliance Requirements

This document is intended to inform the configuration, deployment, and use of all new mobile devices and related services. Compliance with this document is mandatory due to the high degree of vulnerability associated with mobile devices that are deployed and operated without appropriate safeguards.

2. Technical Specification

2.1. Background

The Management and Use of Information & Information Technology (I&IT) Directive requires that Government of Ontario employees protect information that is received, created, held by, or retained on behalf of, Ontario ministries and agencies. Programs are responsible for the implementation of appropriate safeguards, based on an assessment of the risks involved.

Several concerns exist with respect to the use of mobile devices, including but not limited to the following:

- The reduced size of many mobile devices may increase the likelihood of loss or theft;
- The degree of mobile device and/or service authentication may be inadequate;
- Sensitive stored information may be compromised if a device is misplaced or stolen;
- Wireless communications protocols may be intercepted or disrupted;
- Devices will be used outside physical and network perimeters, on public networks; and
- Connection of devices to other equipment may result in the transfer of malicious software.

The features that make mobile devices useful and attractive to users (e.g., compact dimensions, storage capacity, connectivity options, and wireless networking) may represent vulnerabilities if safeguards are not in place.

The implementation of security measures on mobile devices does not diminish the need for Program Managers to ensure that formal, documented risk assessments (e.g., TRAs) are conducted, users are adequately trained, and that safeguards have been implemented to protect Government assets.

2.2. Education and training

Staff responsible for the deployment of mobile devices **must** be aware of the risks inherent in their use, and the security safeguards that **must** be implemented to mitigate these risks.

All Government users of mobile devices **must** be aware of:

- The sensitivity of program information and/or applications as established in accordance with the Information Security & Privacy Classification (ISPC) Policy, to identify any program information that cannot be accessed by, or stored on mobile devices; and
- Their responsibilities for ensuring that mobile device security safeguards are in place, and for following procedures and best practices to avoid unauthorized access to a mobile device or information it may contain.

2.3. Management of mobile devices

All mobile devices used by members of the Ontario Public Service for business purposes **must** be procured through a recognized Government procurement process in areas serviced by a Vendor of Record. All procured devices **must** meet the security requirements identified in this standard. These devices **must** be procured for Government business (or manager-approved uses) only.

Mobile devices that require traditional operating system software for their operation **must** be managed as IT assets and included in patch management operations.

The management of deployed mobile devices **must** include:

- Ensuring that all required security safeguards are appropriately configured and properly maintained;
- Providing mobile device users with instruction/information on procedures and best practices in keeping with the guidance in this standard;
- Establishing secure procedures for maintenance, repair, replacement or return of devices (e.g., secure deletion of information before a device is returned to the vendor or technical staff) where this capability exists; and
- Securely disposing of mobile devices that are no longer required or appropriate for use (see GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media, and associated operating procedures[2]).

Any access to Government of Ontario networks/systems, or a Government mobile service, **must** be immediately deactivated for devices that are reported as lost or stolen. Before access is reactivated for lost or stolen devices (e.g., in the instance where it has been recovered), the identity of the user **must** be positively verified via a secure mechanism or face to face validation.

2.4. Use of mobile devices

The responsible Director or a delegate **must** approve the use of mobile devices in cases where High Sensitivity information may be accessed or stored by the mobile device. The decision to permit such use **must** be informed (and documented) by the relevant program Threat/Risk Assessment (TRA).

The use of mobile devices for processing or storage of High Sensitivity information (including temporary storage) is discouraged.

Government programs that authorize the use of mobile devices for High Sensitivity information **must** first ensure that:

- A documented business case, approved by the responsible program Director, exists for such use and provides a rationale for such operation;
- All required minimum security safeguards are in place, including any additional safeguards recommended by the relevant program TRA;

[2] The GO-ITS 25.20 standard and operating procedures for Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media can be found at: http://intra.net.gov.on.ca/iit/services/iit-policies/

- Users are aware of the sensitivity of the information, restrictions on the use of the device, practices that must be followed to protect the information, and procedures for the secure disposal of sensitive information; and
- Appropriate cryptographic protection is enabled for stored and/or transmitted sensitive information, as defined by GO-ITS 25.12 Use of Cryptography.
- All users of mobile devices **must** protect Government information and the devices by following proper procedures and best practices. Users **must**:
  - Avoid storing unnecessary sensitive information on mobile devices;
  - Keep sensitive information and mobile devices on their person or within sight at all times, or locked in a secure area/compartment, when not at a physical Government location;
  - Maintain awareness of their surroundings when using mobile devices in public areas, to reduce the likelihood of eavesdropping or “shoulder surfing”;
  - Use and store mobile devices at home (e.g., when conducting telework) in an appropriate fashion, such that they cannot be accessed by unauthorized users when unattended;
  - Never use cellular[3] voice/data communication capability (on mobile devices that offer it), SMS messages, or peer-to-peer[4] communication protocols for the transmission of sensitive information;
  - Use Government-issued mobile devices exclusively for Government business purposes;
  - Perform required operations to ensure mobile computer (e.g., notebook, tablet PC) software is functioning correctly and updated;
  - Securely and routinely remove sensitive information from mobile devices when the information is no longer required; and
  - Promptly return mobile devices (to the relevant issuing group) if they are no longer required or appropriate for business purposes.

2.5. Cellular devices

Cellular phones (and any device that supports cellular network voice calls) are ubiquitous within Government but **must** be used appropriately.

Cellular phones[5] do not adequately protect the confidentiality of communications. These devices **must** not be used to communicate or distribute sensitive information (including both voice and data communications).

Use of cellular phone models that support removable media obligates users to familiarize themselves with the security requirements for removable media in this document (and other

[3] Cellular voice communications protocols (e.g., GSM, CDMA) are vulnerable to interception.

[4] Peer-to-peer communication (e.g., RIM BlackBerry PIN-to-PIN) does not leverage centralized security mechanisms, and **must** not be used for sensitive communications. If a BlackBerry device is reassigned, a PIN-to-PIN message intended for its previous owner would be received by its new owner.

[5] For more information regarding cellular device security, please consult NIST special publication 800-124: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

security standards). The requirements described in section 2.3 (regarding sensitive information) apply to such devices.

2.6. Bluetooth

The Bluetooth protocol[6] does not include inherent safeguards sufficient to permit for the transmission of sensitive information. Bluetooth networking (including the use of wireless Bluetooth/RF keyboards) **must** not be used in an environment where sensitive information will be transmitted, received, stored, or processed.

Attack techniques exist that target Bluetooth devices and services. Bluetooth support should be disabled on mobile devices, unless a specific business requirement can be demonstrated and has been endorsed by the program Manager.

Bluetooth audio headsets may be used in conjunction with cellular devices via the Bluetooth *headset* profile. Headset devices **must** not be used for the transmission of sensitive information via voice conversation. Any cellular device used in conjunction with the *headset* profile should be configured such that the device is not permanently visible (e.g., "discoverable") to other Bluetooth devices. Other Bluetooth profile types should be disabled unless a specific business requirement exists for use of an additional profile.

The intended limited operating range of Bluetooth devices **must** not be considered to be a technical safeguard.

2.7. Portable computers

Safeguards **must** be enforced for all mobile computers, both to guard against their use as a platform to attack Government I&IT assets, and to provide sufficient protection for any sensitive information they may store or process. Portable computers **must**:

- Enforce a password implementation that complies with the password requirements described in GO-ITS 25.0 General Security Requirements;
- Restrict the installation of additional software to authorized individuals;
- Implement a centrally managed data encryption capability that complies with the requirements described in GO-ITS 25.12 Use of Cryptography;
- Be configured with centrally managed anti-malware software approved for Government use, with all components maintained to current signature, update, patch, and/or revision levels;
- Not automatically connect to 802.11 wireless local area networks (WLANs) unless specific user input/direction is provided to the system to initiate a WLAN association (e.g., the device **must** not automatically associate); and
- Have 802.11 *ad hoc* wireless support disabled to reduce the potential for unauthorized access via the wireless adapter.

[6] For more information regarding Bluetooth protocol security and Bluetooth devices, please consult NIST special publication 800-121 rev. 1: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

Portable computers that will be used to access the Internet and/or wireless networks **must** have a personal firewall installed that is approved for Government use. The requirements for personal firewalls are described in GO-ITS 25.6 Security Requirements for Firewalls.

Portable computers that are used to remotely connect to Government of Ontario services via Virtual Private Network (VPN) and/or Remote Access Services (RAS) connections **must** comply with GO-ITS 25.7 Security Requirements for Remote Access Services. If such systems are used to connect to a Government operated WLAN service, the portable computer **must** also comply with configuration and use requirements described in GO-ITS 25.5 Security Requirements for Wireless Local Area Networks.

Portable computers to be used to store and/or process sensitive information **must** be configured with additional safeguards (and as required by ISPC and/or a relevant TRA). The additional safeguards **must** include the following:

- Full volume encryption of a type and strength endorsed by SCS in accordance with GO-ITS 25.12 Use of Cryptography;
- Support for secure communication between the portable computer and any relevant networks or applications where transfers or transactions involving sensitive information will occur; and
- Authentication to the portable computer.

In accordance with the requirements stated in GO-ITS 25.0 General Security Requirements, if a portable computer must be accessed by multiple users who share the device, each authorized user of the portable computer **must** have a unique account and credentials to gain access to the device. The user directories, folders, and/or profiles associated with each authorized individual (e.g., on the local storage device) **must** be accessible only to that individual via secure configuration (e.g., local access control lists).

2.8. Integrated handheld/PDA devices

The following mandatory safeguards apply to all integrated handheld and PDA devices:

- Password use **must** be enforced such that access to the device requires authentication;
- Password implementations **must** comply with GO-ITS 25.0 General Security Requirements;
- Processed sensitive information **must** be encrypted in accordance with GO-ITS 25.12 Use of Cryptography;
- Sensitive information should generally not be stored on integrated handheld or PDA devices – exceptions **must** be managed in accordance with section 2.3 of this document;
- General data transmission capabilities should be disabled when the integrated handheld or PDA is connected to a specific communication channel for Government use;
- The device **must** block the use of revoked or expired digital certificates, or

certificates of unknown status[7], for the encryption of messages;

- TLS and/or SSL client capability on the integrated handheld or PDA **must** be configured to deny weak cipher suites (in accordance with GO-ITS 25.12 Use of Cryptography) and connections to servers that present invalid or compromised digital certificates;
- CSB should endorse security and communications software used for integrated handhelds and PDAs; and
- Use of integrated handheld or PDA models that support removable media obligates users to familiarize themselves with the security requirements for removable media in this document.

2.9. Removable media

Removable media includes USB memory (in the form of fobs or “stick” devices), portable hard drives, removable flash media cards (e.g., Compact Flash, Secure Digital cards), and optical disc formats.

All sensitive information stored on removable media **must** be protected by encryption that meets the security and management requirements described in GO-ITS 25.12 Use of Cryptography.

To reduce the risk posed to I&IT assets by malware, removable media **must** be scanned by anti-malware software both upon initial insertion into a portable or desktop computer (e.g., using an “on-demand scan” function or via automated scanning), and when data on the removable media device is accessed.

2.10. Implementation and management of mobile services

All Government infrastructure intended to support or enhance a mobile data communication service for mobile devices **must** be:

- An approved solution that meets GO-ITS 25 series security requirements, and those stated in other relevant GO-ITS documents;
- Installed in an operating environment that is consistent with GO-ITS 25 series security requirements and is endorsed by SCS;
- Deployed and configured in a manner that restricts access to other infrastructure components and networks via the mobile service;
- Properly hardened against attack, managed, and maintained (via proper system and security configuration and provisioning); and
- Subject to intrusion detection/prevention techniques, security testing and evaluation (STE), and compliance audit(s).

[7] Certificates with unknown status are those issued by an unknown or potentially unreliable Certificate Authority (CA), or those that cannot be checked against via the issuers Certificate Revocation List (CRL).

The management of a Government mobile service **must** include:

- Regular updates to all operating system, application, and other software comprising and/or supporting the mobile service, particularly when required to address security vulnerabilities;
- The establishment of procedures and processes to ensure ongoing compliance with the requirements in this document, and other GO-ITS 25 series security standards;
- Prompt reporting and remediation of suspected security breaches and failures to comply with security requirements; and
- Ensuring that new applications for mobile use employ all required safeguards, and are reflected in an updated or new Threat/Risk Assessment for the service.

3. Appendix A: Specific device types

The requirements in this section are specific to the indicated types or classes of devices. These requirements are stated as additional requirements to those outlined in this standard.

RIM BlackBerry Devices

A managed enterprise deployment of RIM BlackBerry services[8] is the intended BlackBerry infrastructure for business use within the Government of Ontario. The current central BlackBerry Enterprise Server (BES) implementation provides this infrastructure, and should be used.

BlackBerry devices **must** employ password protection in accordance with GO-ITS 25.0 password management and use requirements.

Device specific, or *PIN-to-PIN* messages, **must** not be used to communicate for Government business purposes. These messages lack the security safeguards associated with the BES infrastructure.

Individual employees with a business requirement to send or receive High Sensitivity information via the managed BlackBerry infrastructure **must** enable content protection safeguards. The content protection functionality **must** include data encryption of a type and strength determined by SCS to be adequate to protect High Sensitivity information. Any BES configuration enforced on mobile devices **must** support the requirements stated in this policy, and comply with the requirements described in GO-ITS 25.0 General Security Requirements and GO-ITS 25.12 Use of Cryptography.

All browser traffic from user devices should be routed via the managed BES.

Managed BES servers and associated infrastructure **must** be protected from malicious software by centrally managed, approved anti-malware software. Signatures, patches, and revision levels **must** be kept current.

Log information generated by the BES infrastructure **must** be retained in accordance with the requirements stated in GO-ITS 25.0 General Security Requirements. The content of log information associated with BES and user devices **must** also comply with GO-ITS 25.0 General Security Requirements.

Deployed BlackBerry devices reported as lost or stolen **must** have any stored information remotely deleted immediately upon notification, and be remotely deactivated. Devices no longer required or appropriate for use should be securely disposed per the GO-ITS 25.20 standard and procedures for the Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media.[9]

[8] Unmanaged BlackBerry platforms (e.g., Internet Edition) are unacceptable for use; sensitive information cannot be safeguarded, due to a lack of central management for Internet Edition handheld devices and reduced levels of data encryption.

[9] Because PIN numbers are specific to individual BlackBerry devices, someone other than the intended recipient could receive device-specific messages on a device that has been reassigned. For this reason, BlackBerry devices should not be returned to the vendor for reassignment.

4. Related Standards

4.1. Impacts to Existing Standards

Identify any Standards that reference or are referenced by this Standard and describe the impact.

GO-IT Standard	Impact	Recommended Action
GO-ITS 25.0 GO-ITS 25.12 GO-ITS 25.20	Requirements now contained in GO-ITS 25.0 that pertain to mobile device passwords were previously adjusted to accommodate RIM BlackBerry password issues. GO-ITS 25.12 deals with cryptographic requirements for all devices in the Government of Ontario; there are linkages between those requirements and devices described in this standard, but no impact as these documents have been aligned. GO-ITS 25.20 is referenced, but no impact is noted.	Compliance with the standard is recommended.

4.2. Impacts to Existing Environment

Impacted Infrastructure	Impact	Recommended Action
Mobile devices	Adherence to these security requirements will reduce the risks to Government I&IT resources.	Compliance with the standard is recommended due to the current level of risk and impact associated with mobile devices.
Mobile devices	Adherence to these security requirements will reduce the risks to Government I&IT resources and enhance protection for sensitive information when stored and/or processed on mobile devices. Some impact may result with regard to the usability or processing capability of some devices, but this impact is considered to be low. Legacy USB devices may need to be replaced to enable sensitive data storage.	Compliance with the standard is recommended due to the current level of risk and impact associated with mobile devices and removable media.

4.3. Normative References

GO-ITS 25.0 General Security Requirements:
https://www.ontario.ca/government/information-technology-standards#section-6

GO-ITS 25.12 Use of Cryptography:
https://www.ontario.ca/government/information-technology-standards#section-6

GO-ITS 25.20 Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media:
https://www.ontario.ca/government/go-its-2520-disposal-loss-and-incident-reporting-computerized-devices-and-digital-storage

Management and Use of Information & Information Technology (I&IT) Directive:
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.04.11.09.46.33.J6N_res/$File/ManagementOfITDir.pdf

Corporate Policy on Information and Information Technology (I&IT) Security:
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2011.08.09.10.22.28.JV4_res/$File/corporatePolicyIandITSecurity.pdf

ISPC Policy
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.18.14.34.52.PSU_res/$File/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf

ISPC Procedures
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.15.17.13.16.SVU_res/$File/ISPC%20Operating%20Procedures%20-%20Revised%20Aug-07.pdf

4.4. Informative References

Office of the Ontario Information and Privacy Commissioner Order HO-004:

http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf

ISO/IEC Standards:

http://www.iso.org

NIST Special Publications:

http://csrc.nist.gov/publications/PubsSPs.html

800-124 rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise

800-121 rev. 1 Guide to Bluetooth Security

Responsibilities

All users of mobile devices intended for business use are responsible for:

- Complying with Government of Ontario directives, policies and agreements when using Government equipment and services;
- Avoiding the storage of sensitive data on any mobile device, unless authorized and when endorsed by an approved business case;
- Familiarizing themselves with obligations regarding removable media if using a device that supports this type of storage;
- Ensuring security safeguards installed to protect their mobile device are not disabled or tampered with; and
- Reporting any suspected security breaches to the OPS Service Desk.

Directors

Program directors are responsible for:

- Authorizing the storage and/or processing of high sensitivity information on mobile devices by individual employees, based on their job requirements and a formal assessment of the risks involved (via the relevant program TRA);
- Approving the documenting business cases associated with such use;
- Ensuring that staff members are aware of and adequately trained in their responsibilities as set out in this document;
- Supporting efforts to ensure that security safeguards are deployed to protect Government of Ontario information; and
- Reporting any security exposures or suspected security incidents to the IT Service Desk.

Program Managers

Program managers and project teams are responsible for:

- Ensuring compliance with the requirements in this document;
- Ensuring required security safeguards are in place to protect I&IT assets, including additional safeguards recommended and approved via the PIA and TRA processes;
- Authorizing the storage and/or processing of high sensitivity information on mobile devices by individual employees, based on their job requirements and a formal assessment of the risks involved (via the relevant program TRA);
- Approving the documenting business cases associated with such use; and
- Reporting any security exposures or suspected security incidents to the IT Service Desk.

I&IT Clusters

The I&IT Clusters are responsible for:

- Supporting Program Managers and Directors in ensuring that Government information is protected by appropriate security safeguards, and in accordance with both the I&IT Security Directive and ISPC requirements;
- Providing users with instruction and support;
- Ensuring that agreements with service providers address security requirements in instances where a central mobile service is not provided by Infrastructure Technology Services (ITS); and
- Managing assigned mobile devices to ensure they (and any associated services) are used in a manner that adds value with respect to business requirements, and meets these security requirements.

Infrastructure Technology Services (ITS)

ITS is responsible for:

- Ensuring that agreements that they enter into with service providers will reflect the requirements in this document;
- Carrying out any described central management/operations duties for Government mobile devices as outlined in this document;
- Supporting program managers in ensuring that mobile devices are deployed with the required security safeguards in place;
- Providing support and Service Desk services to users of Government mobile devices and services, and supporting security incident reporting and handling procedures;
- Ensuring that the devices and other technical capabilities of the Mobile Network Service Provider can meet the minimum requirements indicated in this document;
- Monitoring the administration, operation and security of all enterprise mobile services supporting Government mobile devices;
- Enforcing BlackBerry Enterprise Server (BES) policy as per the requirements in this document and agreements with SCS; and
- Reporting security incidents to the appropriate Cluster Security Office(s) and I&IT Strategy and Cyber Security Division.

Mobile Network Service Provider

Any Mobile Network Service Provider providing mobile data and/or communication services to the Government of Ontario is responsible for:

- Deploying and operating services in accordance with this standard and relevant GO-ITS 25 series guidance;
- Ensuring network availability for mobile devices and services; and
- Assisting where necessary in the provision of services and/or mobile devices, and ensuring any such services and devices meet the security requirements described in this standard.

I&IT Strategy and Cyber Security Division (SCS)

SCS, or a successor division/branch, is responsible for:

- Authorship of security policies and standards for the Government of Ontario, subject to the approval of the Architecture Review Board (ARB);
- Providing timely guidance on the deployment and use of security products and services to ITS and I&IT Clusters;
- Updating this document and ensuring that mobile security advice and/or requirements are kept current;
- Maintaining this standard and all other applicable IT security standards, policies, procedures and related guidance on behalf of the Government of Ontario;
- Monitoring the evolution of mobile devices and associated technology, assessing relevant vulnerabilities and safeguards, and providing up-to-date security advice to the I&IT Clusters;
- Endorsing mobile device technology and safeguards for use within the Government of Ontario for the communication of sensitive information (e.g., identification of technology and devices that can support required safeguards);
- Operating technical infrastructure associated with supporting cryptography on mobile devices;
- Recommending specific wireless security standards, cryptographic algorithms, and other technical safeguards that are deemed sufficiently secure for use within Government;
- Monitoring for compliance with the requirements in this document in conjunction with ITS;
- Liaising with security authorities at other levels of Government; and
- Managing security incidents.

Ontario Internal Audit

The Ontario Internal Audit Division is responsible for:

- Conducting periodic audits of pertinent activities to test compliance with security standards;
- Communicating with appropriate management about the risks identified and the severity of those risks; and
- Working with management to identify the needed management action plans to mitigate the risks noted during the course of an audit and conducting follow-up as required.

Glossary

Access: Entry to an electronic network provided by the government to its employees and other authorized individuals on or outside government premises, including telework situations.

Accountability: The obligation to answer for results and the manner in which responsibilities are discharged. Accountability cannot be delegated.

Authentication: To establish the validity of a claimed identity of a user prior to gaining access (e.g., passwords, access cards).

Authorize: To grant permission to access resources according to a predefined approval scheme.

Availability: The degree of readiness expected of information systems and IT resources to deliver an appropriate and timely level of service, regardless of circumstances.

Bluetooth: A low power, packet-based RF protocol, operating at approximately 2.4 GHz, intended to replace serial connections and other types of cable connections between small devices.

Confidentiality: Ensuring that information is accessible only to those authorized to have access. Unauthorized disclosure of the information constitutes a loss of confidentiality. The protection of confidentiality must be consistent with the sensitivity of information and legislative requirements (e.g., FIPPA, PHIPA).

Cryptography: The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, detect unauthorized modification, or prevent its unauthorized use. Cryptography is commonly used to provide confidentiality, integrity, message authentication, identity authentication and digital signatures.

Data: Any formalized representation of facts, concepts or instructions suitable for communication, interpretation or processing by a person or by automatic means.

Digital signature: A cryptographic technique based on a uniquely related pair of keys where one key is used to create a signature (the private signing key) and the other to check the signature (the public verification key). A digital signature enables the recipient to verify the source (e.g., the signer) of a message or document and confirm its integrity.

Encryption: The transformation of data via cryptography into a form unreadable by anyone not in possession of the required key. It can provide for data confidentiality by keeping the information hidden from any individual or entity for which it was not intended.

Firewall: Software or a hardware device that acts as a barrier between two networks and mediates access between those two networks according to an approved set of rules.

Identity: Attributes of an individual determining who the individual is as a unique entity.

Identity authentication: A process that uses a credential(s) to verify the identity of a user who is attempting to access resources and/or services.

Information: The meaning derived from or assigned to facts or data, within a specified context.

Information technology assets: Those resources (hardware, software, data etc.) associated with the creation, storage, processing and communication of information in the form of data, text, image and voice.

Integrity: The property that information has not been modified or deleted in an unauthorized and undetected manner.

Malware: Software and/or program code/instructions inserted into a system, usually covertly, with the intention of compromising one or more of confidentiality, integrity, or availability associated with the system or the data it processes. This includes traditional “virus”, “trojan”, and “worm” software as well as “sniffer”, “logger”, “backdoor”, “trapdoor”, and “rootkit” threats.

Network: IT systems that can be made of one or both of the following components:

- Local Area Network (LAN) - Network of Information technology systems wholly situated at one geographical address;
- Wide Area Network (WAN) - located over more than one geographical site.

Password: A string of characters (letters, numbers and other symbols) that are used to authenticate an identity or to verify access authorization.

Pass phrase: A lengthy string of characters intended to provide for significantly increased complexity compared to traditional passwords, in a format users can readily recall from memory.

Privacy: The ability of an individual or group to control personal information and prevent it from being used by people or for purposes other than those they consented to when they provided the information. Organizations must have controls to restrict the collection, use and/or disclosure of personal information to that authorized by the individual or group. In the case of Government organizations, legislative authority is required to collect and use the personal information needed for the delivery of a specific program or service.

Program: A specific program or service within a Ministry.

Program manager: The person responsible for the continued development, operational control, implementation, monitoring, etc. of a specific program or service within a Ministry.

Responsibility: The obligation to perform a given task or tasks associated with a specific role.

Risk: An estimation of the likelihood and impact of potential events on an organization’s ability to meet its business objectives.

Safeguard: A protective and precautionary measure intended to prevent a threat agent from reducing security or causing harm.

Security: The effort to create managed environments within which agents can only perform authorized actions and gain prescribed access, once appropriately authenticated.

Security Testing and Evaluation (STE): A term describing components that comprise the practice of technical security assessment, including (but not limited to) vulnerability assessment, penetration testing, code review, and application testing.
Sensitive Information: Information that if released without authorization would cause harm, embarrassment, or unfair economic advantage, e.g., a breach of confidentiality of personal information, unauthorized modification of financial data, or a release of pre-budget information and strategic planning documents (as determined by ISPC).

Telework: Authorized remote work and computing done for Government purposes, conducted from an employee's home or an alternate location.

Threat risk assessment (TRA): A tool to assist Program Managers in fulfilling their responsibilities for security risk management and the development of security plans. A Threat Risk Assessment (TRA) is used to:

- Assess the sensitivity of program assets and information;
- Identify and analyse potential threats and vulnerabilities;
- Assess the level of risk taking into consideration the effectiveness of current security measures; and
- Recommend appropriate measures to protect assets and information from loss, theft, destruction, modification, or misuse.

User: A person authorized to access and use Information and Information Technology resources.

Virtual Private Network (VPN): A communications session tunneled through another network, and dedicated for a specific use. One common application is secure communication through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. Some types of VPN, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

Acronyms

The following abbreviations and acronyms are used in this standard:

BES: BlackBerry Enterprise Server

CDMA: Code Division Multiple Access

CSB: Corporate Security Branch (MGS)

FRS: Family Radio Service

GMRS: General Mobile Radio Service

GSM: Global Service for Mobile (Communications)

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

ISPC: Government of Ontario Information Security and Privacy Classification Policy

ITS: Infrastructure Technology Services

NIST: National Institute of Standards and Technology (US)

OPS: Ontario Public Service (the employees of the Government of Ontario)

PIA: Privacy Impact Assessment

RAS: Remote Access Services

RF: Radio Frequency

RFID: Radio Frequency Identification

SCS: I&IT Strategy and Cyber Security Division

SMS: Short Message Service

STE: Security Testing and Evaluation

TBS: Treasury Board Secretariat

TRA: Threat Risk Assessment

UHF: Ultra High Frequency

VHF: Very High Frequency

VPN: Virtual Private Network

WLAN: Wireless Local Area Network