Communications Security Establishment
Centre de la sécurité des télécommunications

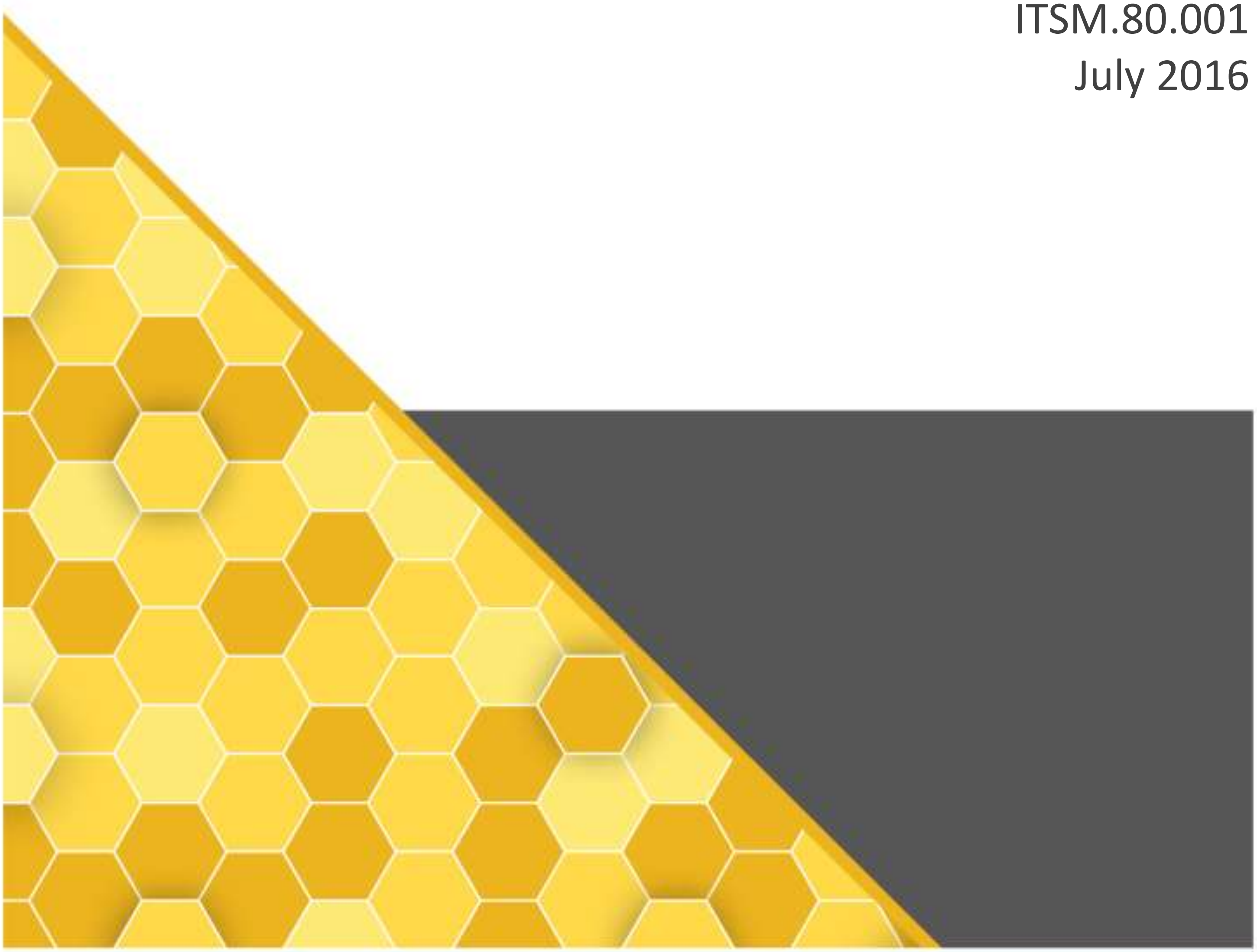
MANAGEMENT SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

SECURING THE ENTERPRISE FOR MOBILITY

ITSM.80.001

July 2016



INTRODUCTION

Mobile devices are a key component for Government of Canada (GC) departments and agencies and have spread rapidly across the GC corporate enterprise. Mobile devices, such as smartphones, tablets, and laptops contain powerful computing capabilities and have the ability to communicate via Wi-Fi, cellular, and Bluetooth. Due to the enhanced functionality of mobile devices, GC employees are using mobile devices to replace paper, to take notes in meetings, and to read documents while travelling.

Today's mobile devices are powerful computers that enable collaboration, and while they boost productivity and efficiency, they can increase the risk of a compromise of sensitive GC information. The security risks are numerous, and must be carefully considered, clearly understood, and security controls and safeguards put in place before mobile devices are allowed to access a departmental network.

This publication provides an overview of Enterprise Mobility Security and lists some of the threats and risks that mobile devices pose to the GC corporate enterprise. This publication also outlines the potential mitigations and safeguards that a department or agency can put into place to counter these threats and risks. It is important to note that these lists are not comprehensive, and even if all possible mitigations have been properly implemented, a residual risk to the department's network and information assets remains.

POLICY DRIVERS

Addressing and countering cyber threats, risks, and vulnerabilities GC networks are facing is crucial to securing GC networks, data, and assets. As such, GC departments must ensure IT security policies and procedures are implemented in accordance with the following Treasury Board of Canada Secretariat (TBS) policies:

- *Policy on Management of Information Technology* [1][1];
- *Policy on Government Security* [2]; and
- *Operational Security Standard: Management of Information Technology Security (MITS)* [3].

APPLICABLE ENVIRONMENTS

The information in this publication provides guidance for IT solutions at the UNCLASSIFIED, PROTECTED A, and PROTECTED B levels. Systems operating in the PROTECTED C or Classified domains may require additional design considerations that are not within the scope of this document[2]. It is the department's responsibility as part of a risk management framework to determine the security objectives required to protect departmental information and services.

[1] Numbers in square brackets indicate reference material which is listed in the Supporting Content section.

[2] Contact CSE COMSEC client services for guidance regarding IT solutions in the PROTECTED C or Classified domains.

ENTERPRISE MOBILITY BUSINESS DRIVERS

GC employees make up a world-class workforce that requires access to the latest technologies to perform their tasks and ensure GC departments reach their goals. To aid in this endeavour, mobile technologies are being used by an increasing numbers of employees for the following reasons:

- **Ease of use** - Mobile devices have user-friendly interfaces that can be customized to meet the needs of both the employee and the GC;
- **Anytime, anywhere connectivity** – GC employees require remote access to business data as well as enterprise services and applications in order to work efficiently and effectively. This is especially important for GC employees who travel frequently;
- **Customization** – Departments can customize device settings to allow convenience and flexibility for the employee;
- **Cloud Computing** – The GC has been moving towards cloud based infrastructures to deliver services; and
- **Cost to the GC** - Mobile device providers are constantly producing higher quality and more powerful devices. The use of mobile devices and service providers minimizes program cost and reduces technical obsolescence issues, as compared with GC specified and developed devices.

ENTERPRISE MOBILITY OVERVIEW

Enterprise Mobility provides GC employees with the ability to access data and departmental services anywhere and at anytime – inside the building, within the city, within Canada, and while on international travel. Remote network access through mobile devices allows employees to collaborate and perform their duties more efficiently and effectively.

Enterprise mobility allows mobile devices, such as smartphones, tablets, and laptops to access a department’s networks and services through the use of commercial cellular networks and Wi-Fi. Figure 1 illustrates the basic segments of the Enterprise Mobility architecture.

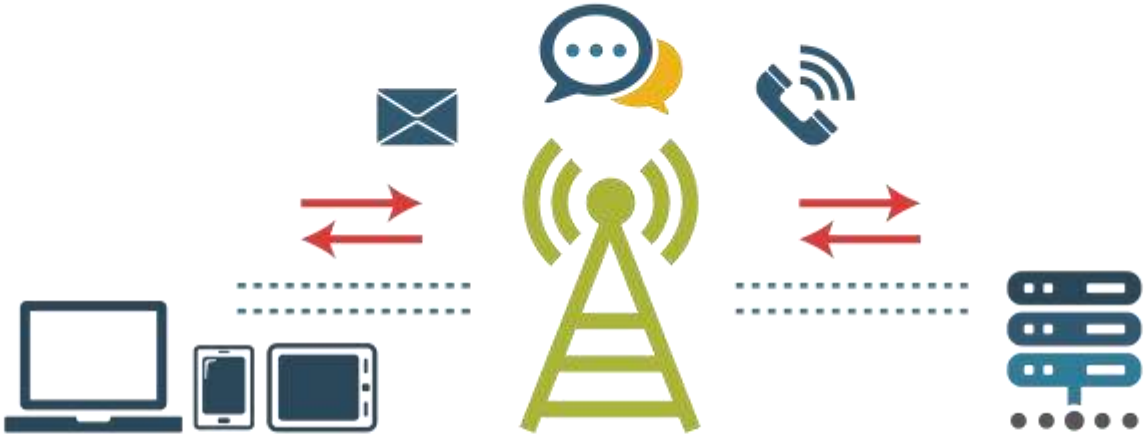


Figure 1 Basic Segments of the Enterprise Mobility Architecture

MOBILE DEVICES

Mobile devices are commercial products, and include smartphones, feature phones, tablets, and laptops, that support connection to GC networks. Mobile devices are widely available, cost effective, and contain up-to-date technology for communications and application functionality. Mobile device features are constantly changing, but contain the ability to make wireless network connections for voice and data communications, memory, a GPS, and digital and video cameras.

WIRELESS COMMUNICATIONS NETWORKS

Major types of wireless networks include:

- **Cellular networks -** managed by commercial carriers and provide coverage based on dividing a large geographical service area into smaller areas of coverage;
- **Wi-Fi networks -** may be established by businesses or consumers to provide a networking service within a limited geographic area, such as a home, office, or place of business; and
- **Other wireless networks -** may not conform to the Wi-Fi standard. For example, Bluetooth is often used to establish connectivity with nearby devices, such as headsets or computer keyboards.

GC ENTERPRISE INFRASTRUCTURE

The GC Enterprise Infrastructure provides hardware, software, network resources, and services required for the existence, operation, and management of an enterprise IT environment. It enables the GC to deliver IT solutions and services to its employees, partners, and clients. Mobility-specific applications may also be hosted on the GC Enterprise, or the ability to interact with other mobile devices may be provided. The enterprise mobility capability can secure and manage the interaction between GC enterprise services and authorized devices and users.

SERVICES AND APPLICATIONS

Services and applications are the existing and evolving services provided for all enterprise users, including mobile users. GC enterprise services include unified communications such as data (e-mail and chat), voice (telephone and teleconferencing), and applications and/or web interfaces.

IT SECURITY RISK MANAGEMENT

The use of mobile devices, wireless networks, and voice and data services exposes the GC to a number of threats. These threats include actions that can be deliberate or accidental, taken by an adversary or by an authorized user. They need to be addressed and sufficiently mitigated to achieve acceptable risk levels. There are a number of mitigation strategies for threats associated with Mobility, and most of these strategies work in concert with one another. In particular, the Enterprise Mobility Infrastructure and existing Enterprise capabilities can provide strong security features to protect mobile devices and employee communications.

THREATS AND RISKS

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices (e.g., desktop and laptop devices only used within the organization's facilities and on the organization's networks). Major security concerns for these technologies include the following:

- Lack of physical security controls;
- Use of untrusted mobile devices;
- Use of untrusted networks;
- Use of untrusted applications;
- Interaction with other systems;
- Use of untrusted content; and
- Use of location services.

Since the threats posed by mobile device use are numerous, they must be clearly understood and mitigated to protect the confidentiality, availability, and integrity of GC information. Some principal threats include:

DEVICE THREATS AND RISKS

- Identifying, targeting, and delivering malware to a device;
- Using the network connections of the device (cellular, Wi-Fi, Bluetooth) for nefarious purposes;
- Using the device to infiltrate other GC networks;
- Accessing the device to track location through GPS;
- Activating the microphone or camera;
- Intercepting voice and data communications;
- 3rd party software gaining access to device features;
- Unauthorized device modification, including changing the hardware or software of the mobile device either remotely, with physical access, or within the supply chain; and
- Software flaws, out-of-date Operating Systems.

INFORMATION CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY THREATS AND RISKS

- Exfiltration or monitoring of sensitive voice or data communications via Bluetooth, Wi-Fi, or other means;
- Sensitive data being stored unprotected on a mobile device; and
- Denial of Service attacks.

ENTERPRISE THREATS AND RISKS

- Loss of authentication credentials such as passwords or private keys for certificates;
- Improper disposal of old mobile devices with sensitive configurations and/or data;
- Use of social media applications contrary to policy;
- Lost or stolen device attempting to access the Enterprise Mobility Infrastructure or masquerade as authorized users;
- Authorized equipment users attempting to misuse their privileges, such as by trying to use disallowed services/applications or trying to connect directly to commercial services; and
- Untrusted apps stores that repackage versions of popular apps that include malware.

THE IT SECURITY RISK MANAGEMENT PROCESS

CSE's *IT Security Risk Management: A Lifecycle Approach (ITSG-33)* [4] guidelines suggest a set of activities at two levels within an organization; the departmental level and the information system level. Departmental level activities are integrated into the organization's security program to plan, manage, assess and improve the management of IT security-related risks faced by the organization. Once overall roles and responsibilities are defined, the guidelines in Annex 1 of ITSG-33 [4] further suggest and describe IT security risk management activities to define, deploy, monitor, assess the performance of, and update security controls across a department. The execution of these activities follows a standard lifecycle process to be integrated into the overall departmental security program.

Information System level activities are integrated into an information system lifecycle to ensure IT security needs of supported business activities are met, appropriate security controls are implemented and operating as intended, and continued performance of the implemented security controls is assessed, reported back and acted upon to address any issues. The guidelines found in Annex 2 of ITSG-33 [4] suggest IT security risk management activities to implement, operate, and maintain dependable information systems. These activities apply to the life cycle of information systems, which consist of phases for their implementation, operations and maintenance, and disposal. To assist departments, Annex 2 of ITSG-33 [4] suggests a secure System Development Lifecycle (SDLC) process referred to as the Information System Security Implementation Process (ISSIP).

MITIGATION STRATEGY

Departments should use a defense-in-depth strategy in which multiple layers of security are placed throughout an IT system to provide redundancy in the event a security control fails or a vulnerability is exploited. To protect sensitive GC information and GC networks, GC departments should implement the following layered, defense-in-depth strategy. The strategy has three layers which has a balanced focus on three primary elements: people, technology and operations.

1. DEPARTMENTS SHOULD HAVE A MOBILE DEVICE SECURITY POLICY

The departmental mobile device security policy should define which resources may be accessed via mobile devices, the degree of access that mobile devices may have, and which types of mobile devices are permitted to access departmental resources (e.g., GC-issued devices versus personally-owned devices). The security policy should also cover how mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies. The mobile device security policy should be documented in the departmental security plan.

2. DEPARTMENTS SHOULD HAVE AN EMPLOYEE TRAINING AND AWARENESS PROGRAM IN PLACE

Information security is the responsibility of everyone in the organization. Employee responsibility should be clearly defined, communicated, and supported with effective education and awareness. It only takes one malicious e-mail attachment to be opened or one malicious website to be accessed to compromise an entire network. Employee diligence and dedication is an important factor for business continuity in the face of today’s cyber threats; consequently, awareness should be supported by senior management and be part of the strategic framework.

3. DEPARTMENTS SHOULD PERFORM THREAT AND RISK ASSESSMENTS FOR MOBILE DEVICE USE

Mobile devices often need additional protection because their mobile nature exposures them to more threats than other devices. Before designing and deploying mobile device solutions, departments should perform Threat and Risk Assessments (TRAs). TRAs help departments identify security requirements and design the mobile device solution so that it includes the security controls needed to meet the security requirements. TRAs involve identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added.

4. DEPARTMENTS SHOULD ENSURE THE NECESSARY SECURITY SERVICES ARE EMPLOYED

Departments should consider the merits of each security service, determine which services are needed, and then employ the solutions that provide the necessary services. Services that should be considered include the following:

- **Departmental security policy:** enforcing departmental security policies on the mobile device, such as restricting access to hardware and software, managing wireless network interfaces, and automatically monitoring, detecting, and reporting when policy violations occur;
- **Data communication and storage:** supporting strongly encrypted data communications and data storage, wiping the device before reissuing it, and remotely wiping the device if it is lost or stolen;
- **User and device authentication:** requiring device authentication before allowing the mobile device to access departmental resources; and

- **Third-party Applications:** restricting which applications may be installed, determining the permissions assigned to each application, and verifying digital signatures on applications.

5. DEPARTMENTS SHOULD TEST A PILOT OF THEIR MOBILE DEVICE SOLUTION

Aspects of the solution that should be evaluated for each type of mobile device include connectivity, protection, authentication, application functionality, solution management, logging, and performance. All components of the system should be updated with the latest patches and configured following sound security practices.

6. DEPARTMENTS SHOULD SECURE GC-ISSUED MOBILE DEVICES BEFORE ALLOWING USER ACCESS

Fully securing each device before allowing users to access the device ensures a basic level of trust in the device before it is exposed to threats. Any previously deployed GC-issued mobile devices with unknown security profiles should be fully secured to a known good state through mobile device management technologies. Supplemental security controls should be deployed as risk merits, such as anti-virus software and Data-Loss Prevention (DLP) technologies.

7. DEPARTMENTS SHOULD REGULARLY MAINTAIN MOBILE DEVICE SECURITY

Departmental security processes for maintenance include:

- Ensuring upgrades and patches are installed;
- Reconfiguring access control features when required;
- Detecting and documenting anomalies within the mobile device infrastructure, including unauthorized configuration changes to mobile devices;
- Keeping an accurate inventory of each mobile device, its user, and its applications;
- Revoking access to or deleting an application that has been assessed as too risky to use; and
- Scrubbing sensitive data from mobile devices before reissuing them.

Departments should periodically perform audits to ensure that their mobile device policies, processes, and procedures are being followed properly.

CSE’S MOBILITY SUITE

To help mitigate the threats posed by mobile device, CSE has put together a suite of Mobile Security publications that when applied can help GC departments significantly reduce their threat surface in regards to mobile devices. Visit www.cse-cst.gc.ca/its to download:

- Mobile Technologies in International Travel;
- CSE’s Top 10 Security Actions;
- Mobile Device Management Solutions;
- IT Security Risk Management: A Lifecycle Approach;
- Security Requirements for Wireless Local Area Networks;
- Security Considerations for Exposure of Classified IT Systems to Mobile Devices and Wireless Signals;
- Mobile Security – Securing the Government of Canada; and
- Using Your Mobile Device Securely.

SUMMARY

Mobile devices are convenient, flexible, and allow employees to work anywhere and at anytime, but their complex design and enhanced functionality can pose a threat to GC information, its assets, and its networks. Since mobile devices can contain, or provide access to, vast amounts of sensitive government and personal information, they are attractive targets that can provide unique opportunities for threat actors intent on gathering information.

Current commercial mobile devices have not fully addressed all security issues relevant to GC operations. Since the threats posed by mobile device use are numerous, they must be clearly understood and mitigated to protect the confidentiality, availability, and integrity of GC information. Enterprise Mobility should use commercially available protections and compensate for device limitations within the overall Enterprise Mobility architecture, leverage the secure GC enterprise, and develop departmental security policies especially for mobile devices. Where necessary, commercial mobile devices may be further hardened to improve integrity and reduce risks.

Even though mobility is a necessary requirement for GC employees, the confidentiality, availability, and integrity of information must be protected. To achieve this, security controls for GC Enterprise Mobility solutions should be determined according to the department’s threat and risk assessment. CSE’s *ITSG-33 IT Security Risk Management: A Lifecycle Approach* defines a security risk management process whereby a pre-defined set of baseline security controls can be tailored to meet the specific security needs of a department. Security controls need to be implemented and verified for the complete information system, from the mobile device through to the departmental network services that support the business processes and information assets.

CONTACTS AND ASSISTANCE

If your department has identified a requirement for Mobility based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

SUPPORTING CONTENT

LIST OF ABBREVIATIONS

Term	Definition
CSE	Communications Security Establishment
GC	Government of Canada
DLP	Data Loss Prevention
GPS	Global Positioning Systems
IT	Information Technology
ISSIP	Information System Security Implementation Process
ITS	Information Technology Security
SDLC	System Development Lifecycle
TBS	Treasury Board of Canada Secretariat

REFERENCES

Number	Reference
1	Treasury Board of Canada Secretariat. *Policy on the Management of Information Technology,* 1 July 2007.
2	Treasury Board of Canada Secretariat. *Policy on Government Security,* 1 July 2009.
3	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology,* n.d.
4	Communications Security Establishment. *ITSG-33 IT Security Risk Management: A Lifecycle Approach,* December 2014.
5	National Security Agency. *Mobility Security Guide*, 4 November 2013.
6	National Institute of Standards and Technology. *Special Publication 800-124 Revision 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013.

7	United States Government Accountability Office. *Better Implementation of Controls for Mobile Devices Should Be Encouraged*, September 2012.
8	United States Computer Emergency Readiness Team. *Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices*, 15 April 2010.