MOBILE COMPUTING SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0
Published: September 2019
## Table of Contents

I  INTRODUCTION, SCOPE, BACKGROUND .................................................................3

II GLOSSARY, TERMS AND DEFINITIONS, LIST OF COMMONLY USED REFERENCES .........................3

1 MOBILE COMPUTING AND TELEWORKING ..................................................................4

1 MOBILE COMPUTING ..............................................................................................4
I  Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

This standard is also designed to be read in conjunction with the Mobile Device Security Standard (published here: IM/IT Standards).

II  Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references” sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.
1 Mobile computing and teleworking

1 Mobile computing

1.1 Appropriate controls must be implemented to mitigate security risks associated with the use of mobile devices.
   a) Information protection paramount
   b) Service-specific risks and practices
   c) Protection of credentials
   d) Protection of network endpoint and physical device
   e) Human factors
   f) Risk assessment factors

Purpose: To protect information stored on mobile devices from loss or unauthorized access.

1.1 a) Information protection paramount
The use of mobile devices such as laptops, tablets or smartphones to access, store, or process information increases the risk of information compromise. Mobile devices are typically small and portable, used in uncontrolled public environments, and easily lost, stolen or damaged.

Information Owners and Information Custodians must ensure that use of mobile devices is managed and controlled. To ensure that sufficient safeguards are implemented to mitigate risks mobile devices must be enrolled in Mobile Device Management Service. Users of mobile devices must protect the information and information technology assets in their custody or control.

1.1 b) Service-specific risks and practices
Providers of mobile computing services (such as Technology Services Division) must perform regular risk assessments to identify service-specific risks (e.g., perform or update the risk assessments on an annual basis). Information Owners and Information Custodians must develop, document and maintain policies, standards, practices and guidelines that address these risks, and communicate them to employees.

1.1 c) Protection of credentials
User identifiers and user credentials must be protected to reduce the risk of unauthorized access to information and information technology assets. In particular, employees must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places.

1.1 d) Protection of network endpoint and physical devices
Mobile devices are typically used to store information or remotely access government networks and services. The policies and procedures governing remote access apply to mobile devices. Where Remote Access services are used, the mobile device must be configured to prevent its use as a conduit between the non-government and government networks (e.g., VPN split tunnelling must be disabled).

Network access to mobile devices from non-government networks must be blocked by implementation of firewall or filtering technologies to protect against attack (e.g., to prevent network attacks against the mobile device).
Mobile devices must be protected against mobile and malicious code. Mobile devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

1.1 e) Human factors
Information Owners and Information Custodians must provide employees using mobile devices with security awareness training to ensure that they are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using mobile devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with the Information Incident Management Process.

1.1 f) Risk assessment factors
The Security Threat and Risk Assessment must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of mobile devices to remotely access Government networks and systems;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device disposal;
- Information disposal;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Information classification and sensitivity levels must be considered in the risk assessment. Storage of government information on mobile devices must be avoided and is allowed only in extenuating circumstances, as defined in the Appropriate Use Policy.

Minimum information protection safeguards for the use of mobile devices must include:

- Encryption of stored data to prevent information loss resulting from the theft of the mobile or remote device;
- Encryption of data transmitted via public network;
- Access control permissions on a mobile device to prevent unauthorized access to information by system users, particularly for multi-user mobile systems;
- Regularly maintained data backups of information stored on mobile devices using government backup facilities to protect against information loss;
- Physical security of the device at all times to protect against asset and information loss; and,
- User authentication to the mobile device and user authentication for remote access from the device in accordance with authentication policies.

Recommended Tests:
Note: 1.1 is reported on as part of the annual information security review.

- Demonstrate that Security Threat and Risk Assessments have been completed on mobile devices.
- Demonstrate that only approved mobile devices are in use.
• Demonstrate that all mobile devices are registered and regularly inventoried.
• Demonstrate that processes are in place to update software and apply patches.
• Demonstrate restricted access and that appropriate access controls are applied.
• Demonstrate that protection mechanisms such as cryptographic controls, malware protection and remote disabling/erasures are applied when available or required.

Additional resources: This standard is also designed to be read in conjunction with the Mobile Device Security Standard (at: IM/IT Standards).