Mobile Device and Telework Security Policy

Last Review: March 2020
Next review: December 2020

Ministry of Central Services
Maintained by: Information Security Division

Purpose

To mitigate risks associated with the use of mobile devices and teleworking.

Scope

This policy applies to all GoS owned or operated information systems, intellectual property, and government records.

Policy Statements

Appropriate security controls must be implemented to mitigate risks associated with the use of mobile devices.

Information Owners must consider the risks associated with the use of mobile devices in unprotected environments. The following are the minimum controls that must be implemented.

The Information Owner must:

- develop, document and implement procedures on the issuance, usage and return of mobile devices;
- ensure that only government-owned or government-managed mobile devices are used on the government network and to store government information;
- ensure all mobile devices are inventoried;
- ensure mobile devices are returned and, where applicable, disposed of in accordance with the Asset Management Policy and Standards;
- ensure that sensitive data on mobile devices is encrypted with approved methods;
- ensure that mobile devices are password-protected and lock automatically after a predetermined number of unsuccessful login attempts or period of inactivity;
- only allow access and storage of information that has a Security Classification of Level A on mobile devices when there is a distinct business requirement;
- ensure software to protect against malicious software is installed and maintained;
- authorize the use of mobile devices during out-of-country travel;
- ensure users are trained on the proper use of mobile devices, associated software and services, and security incident reporting;
- ensure users are informed of and accept the terms and conditions of these standards and related policies; and
- ensure all consultants and IT service provider contracts and agreements include clauses which reference this and other security standards and policies.

Users must:

- have authorization from the Ministry or agency to use mobile device(s);
- ensure that mobile devices in his or her care are only accessed by those authorized to do so;
- ensure that mobile devices are password-protected and the password applied in accordance with the Access Control Security Policy and Standards;
- ensure that mobile devices are not left unattended;
- protect mobile devices from loss, theft, damage and unauthorized access;
- ensure that information that has a sensitivity of Level A is not accessed by or stored on mobile devices unless s/he has received explicit authorization from the Ministry and the Information Owner to do so;
- ensure that all sensitive information transmitted by or stored on mobile devices is encrypted by approved methods;

- backup information stored on all mobile devices in accordance with Ministry standards and policies;
- ensure that information that cannot be stored on the Ministry shared network drive must be saved to media, encrypted by an approved method and transported and stored securely;
- ensure that data on mobile devices are not the only copies that exist;
- ensure that only software authorized for use on the government network is installed;
- ensure that software is installed only by those authorized to do so;
- ensure that sensitive information is not accessed while using mobile devices in a public place (e.g. coffee shop, airport, park); and
- immediately report the loss or theft of a mobile device to the user's supervisor and the Information Technology Division Service Desk.

Appropriate security controls must be implemented to mitigate risks associated with teleworking.
Telework arrangements must be in compliance with the Government of Saskatchewan Telework Policy (Human Resource Manual 1104). Before granting permission to enter into a telework arrangement the Ministry must consider:

- the sensitivity of information accessed or stored at the location;
- the physical security at the teleworking location;
- likelihood of unauthorized access at the teleworking location;
- the security of home wired and wireless networks; and
- remote access threats.

Mandatory controls are:

- sensitive government information in electronic format cannot be stored at a teleworking site unless it is encrypted with approved methods;
- sensitive government information in hard copy format cannot be stored at a teleworking site unless it is in a locked cabinet;
- teleworking sites where Classification Level A information is stored must be monitored by alarm when vacant;
- only government-issued computers can be used for the processing of government information;
- only approved remote access methods can be used to access the government network;
- at least monthly, government-issues computers must be brought to the primary work site, logged into the network and have patches and updates applied; and
- a home wireless network used to access the government network must be secured in accordance Communications and Network Security Policy and Standards.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer. Policy exceptions will be reviewed on a periodic basis for appropriateness.