Physical and Environmental Security Policy

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines Government of Saskatchewan security policy for Physical and Environment Security.

Purpose

To prevent unauthorized physical access, loss, damage, theft, compromise or interference to the government's information, assets, and operations.

Scope

This policy applies to all GoS owned or operated information systems, assets, and operations.

Policy Statements

Secure Areas

Government information processing facilities must be protected by a physical security perimeter.

- Information Owners must ensure appropriate controls are in place to establish secure areas. Sensitive information and assets must be protected while considering the safety of personnel. Control selection must be supported by a Threat and Risk Assessment.
- Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Controls to ensure security of information and information systems located in government offices, rooms and other facilities must be designed, applied and documented. Information Owners and Ministry Security Officers must regularly assess the security of areas where sensitive information is processed and/or stored.

Information Owners, Ministry Security Officers, planners and architects must ensure:

- physical protection against natural disasters, malicious attack or accidents are designed and applied; and
- access points such as reception, delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, if possible, isolated from secure areas or offices to avoid unauthorized access.

Information Owners and Ministry Security Officers must identify and document any additional requirements that apply to personnel who have been authorized to work in secure areas.

Equipment

Information Owners, Ministry Security Officers, planners and architects must ensure that:

- Government facilities are designed in a way that safeguards sensitive information and assets;
- Equipment is protected to reduce the risks from unauthorized access, environmental threats and hazards;
- Equipment is protected from power supply interruption and other disruptions caused by failures in supporting utilities;
- Power and telecommunications cabling carrying data or supporting information services are protected from interception or damage; and
- Equipment is correctly maintained to help ensure availability and integrity of sensitive information and assets.

Information Owners must ensure that:

- Government-owned equipment, information and software is not removed from government premises without prior authorization, and personnel are informed of and accept responsibility for protection of the asset;
- Assets are safeguarded using documented security controls when off-site from government premises; and
- All data and software must be erased from equipment prior to disposal or re-deployment.

Users must ensure that:

- Unattended equipment has appropriate protection;
- They safeguard sensitive information from unauthorized access, loss or damage by securing their work space when it cannot be monitored by authorized personnel; and
- Sensitive information is not discussed in public or other areas where there is a risk of being overheard by unauthorized personnel.

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.