Physical and Environmental Security Policy

Ministry of SaskBuilds and Procurement
Information Technology Division
Cyber Security and Risk Management Branch

Last revised: October 2023
Last reviewed: November 2023
Next review: November 2024

Physical and Environmental Security Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Contents

Physical and Environmental Security Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Purpose

The purpose of this policy is to ensure proper measures are in place to prevent unauthorized physical access, loss, theft, interference or damage to the organization's information and facilities

Scope

This Operations Security Policy applies to all business processes and data, information systems, components, personnel, and physical areas of the Government of Saskatchewan. Person(s) this policy applies to include but are not limited to:

- All employees, whether employed on a full-time or part-time basis by the Government of Saskatchewan
- Contractors and Service Providers that access and manage Government of Saskatchewan assets.

Governing Laws, Regulations, and Standards

Resource	Description
Privacy Act	*P-21.pdf (justice.gc.ca) Government of Canada Privacy Act*
PIPEDA	*P-8.6.pdf (justice.gc.ca)Government of Canada PIPEDA Act*
Freedom of Information and Protection of Privacy Act	Saskatchewan's provincial public sector privacy law
Local Authority Freedom of Information and Protection of Privacy Act	*Saskatchewan's municipal public sector privacy law*
Health Information Protection Act	*Saskatchewan's privacy law relating to health records*
ISO/IEC 27001:2013	11.1.1~11.1.6, 11.2.1~11.2.9
ISO/IEC 27002:2022	7.1~14, 8.1
NIST (National Institute of Standards and Technology) SP 800-53 r5	PE-3~5, PE-16, AU-6(6), PE-3, PE-3(3), PE-6, PE-6(1), PE-6(4), CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23, SC-42, AC-11, MP-2, MP-4, AC-19, AC-20, MP-5, PE-17, MA-2, MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-4, PE-9, MP-6, MA-2, MA-6

Physical and Environmental Security Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Policy Statements

Physical and Environmental Security:

- Physical security perimeters should be defined, and appropriate entry controls should be implemented at secure access points to ensure only individuals with appropriate access levels are allowed access. These access points will be monitored.
- Physical security for offices, rooms and facilities should be designed and implemented. Premises should be continuously monitored for unauthorized physical access.
- Visitors must be identified, logged, and escorted as required.
- Protection against natural disasters or other malicious attacks, as well as accidental incidents, will be determined and implemented.
- The Government of Saskatchewan should place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.
- Applicable security measures will be implemented for offices, boardrooms, etc., including considerations for temperature, protection against water damage, and emergency lighting
- Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Equipment Security:

Information Owners must ensure that:

- Government-owned equipment, information and software are not removed from government premises without prior authorization, and personnel are informed of accepted responsibility for the protection of the assets.
- Assets are safeguarded using documented security controls when off-site from government premises.
- All data and software must be erased from equipment before 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 workspace when it cannot be monitored by authorized personnel.

- Sensitive information is not discussed in public or other areas where there is a risk of being overheard by unauthorized personnel.

Supporting Internal Resources

Resource	Description
Internal Security Governance Policy	All Government of Saskatchewan Security Policies align to this Governance Policy
Information Protection Security Controls (IPSC) for Classified Data	This document defines the required access controls required to provide the proper security based on Classified Data for Government of Saskatchewan
Operations Security Policy	Ensures correct and secure operations of information systems, and that the impact of change activities on operational systems are minimized.

Non-Compliance

In cases where it is determined that a breach or violation of Government of Saskatchewan Information Security policies has occurred, the respective Ministry under the direction of the Chief Information Officer and Information Security Branch, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, in accordance with PS 803 Corrective Discipline policy, 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 a review and acceptance of risk by the Security Governance Committee. Exceptions to this policy must be formally documented and approved by the Chief Information Security Officer, under the guidance of the Cyber Security and Risk Management Branch. Policy exceptions will be reviewed periodically for appropriateness.

Definitions

This section intentionally left blank.

Physical and Environmental Security Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Revision History

Version ID	Date of Change	Author	Rationale
V1.0	October 20, 2023	Final Draft	First Draft
V1.2	November 20, 2023	CSRM	Final Draft