Operations 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: October 2024

Operations Security Policy

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

Contents

This document is intended for the Saskatchewan Ministry of SaskBuilds and Procurement, Information Technology Division, and partner organizations.
It may contain legally privileged and/or confidential information and must not be disseminated, distributed, or copied

Operations Security Policy

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

Purpose

To ensure correct and secure operations of information systems, and that the impact of change activities on operational systems are minimized.

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	12.1.1, 12.1.2, 12.1.3, 12.1.4, 12.2.1, 12.3.1, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 12.5.1, 12.6.1, 12.6.2, 12.7.1
ISO/IEC 27002:2022	5.37, 8.6, 8.7, 8.8, 8.13, 8.15, 8.17, 8.32, 8.19, 8.31, 8.34
NIST (National Institute of Standards and Technology) SP 800-53 v4	AC-1, SI-2,9, RA-5, CP-9, AU-2,3,4,6,8,9,11,12,14, CM-3,5,7,11, SA-3,10,

Policy Statements

- A change management process must be established to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems.
- Process and technology must be in place to monitor and maintain information systems software throughout the software lifecycle.
- Backup and recovery processes must be defined, documented, and assessed on regular basis.
- Process must be implemented for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems.
- Operating procedures and responsibilities for managing information systems and information processing facilities must be documented, authorized, and reviewed on a regular basis.
- Log files must be protected against unauthorized modification, access, or disposal.
- A well-established process must be in place to identify, assess, and respond to vulnerabilities.
- Computer clocks must be synchronized to ensure integrity of information system logs and accurate reporting.

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

Non-Compliance

A breach of this policy may lead to discipline, up to and including termination, in accordance with PS 803 Corrective Discipline policy. Similarly, for contracted resources or entities, Government of Saskatchewan will initiate corrective measures up to and including restricting access to services or initiating disciplinary action up to and including 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.

Revision History

Version ID	Date of Change	Author	Rationale
V1.1	Sept 19, 2023	CSRM	First Draft
V1.2	November 19,2023	CSRM	Final Draft