

# Operations Security Policy

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

## Operations Security Policy

**Ministry of SaskBuilds and Procurement**  
Information Technology Division  
Cybersecurity and Risk Management Branch

Last revised: July 2025  
Last reviewed: August 2025

# Operations Security Policy

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

## Confidentiality Statement

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.

## Contents

CONFIDENTIALITY STATEMENT .....	1
PURPOSE.....	2
SCOPE .....	2
GOVERNING LAWS, REGULATIONS, AND STANDARDS.....	2
POLICY STATEMENTS.....	3
SUPPORTING INTERNAL RESOURCES.....	3
NON-COMPLIANCE .....	3
EXCEPTIONS .....	3
DEFINITIONS .....	4
REVISION HISTORY .....	4

# Operations Security Policy

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

## Purpose

To ensure correct and secure operations of information systems, and that the impact of change activities on operational systems is 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
<i>Privacy Act</i>	<a href="#">P-21.pdf (justice.gc.ca) Government of Canada Privacy Act</a>
<i>PIPEDA</i>	<a href="#">P-8.6.pdf (justice.gc.ca) Government of Canada PIPEDA Act</a>
<i>Freedom of Information and Protection of Privacy Act</i>	<a href="#">Saskatchewan's provincial public sector privacy law</a>
<i>Local Authority Freedom of Information and Protection of Privacy Act</i>	<a href="#">Saskatchewan's municipal public sector privacy law</a>
<i>Health Information Protection Act</i>	<a href="#">Saskatchewan's privacy law relating to health records</a>
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,

# Operations Security Policy

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

## 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 a 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 the integrity of information system logs and accurate reporting.

## Supporting Internal Resources

Resource	Description
Internal Security Governance Policy	All Government of Saskatchewan Security Policies align with this Governance Policy.
Information Protection Security Controls (IPSC) for Classified Data	This document defines the required access controls to provide the proper security based on classified data for the Government of Saskatchewan

## Non-Compliance

In cases where it is determined that a breach or violation of the Government of Saskatchewan Information Security policies has occurred, under the direction of the Chief Information Officer:

- Cybersecurity and Risk Management Branch will initiate technical corrective measures, including restricting access to services;
- Permanent Head or designate may initiate disciplinary action up to and including dismissal, in accordance with PS 803 Corrective Discipline policy; and
- Permanent Head or designate may initiate 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 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 Cybersecurity and Risk Management Branch. Policy exceptions will be reviewed periodically for appropriateness.

# Operations Security Policy

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

## 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