Cloud Computing Security Policy

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

Last revised: July 2025
Last reviewed: August 2025

Saskatchewan

Cloud Computing Security Policy

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

Confidentiality Statement

Contents

Cloud Computing Security Policy

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

Purpose

To ensure that the confidentiality, integrity, and availability of the Government of Saskatchewan's information is preserved when stored, processed or transmitted by a cloud service provider. This policy defines governing regulations, internal and industry standards required to maintain the required controls when delivering projects or programs to the Government of Saskatchewan.

Scope

This Cloud Computing Security Policy applies to all business processes and data, information systems, components, personnel working with cloud services for 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; and
- 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 27002:2022	5.23
NIST (National Institute of Standards and Technology) SP 800-53 v4	SA-1, SA-4, SA-9, SA-9(3), SR-5

Cloud Computing Security Policy

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

Policy Statements

- All Government of Saskatchewan (GOS) information under consideration for use in a cloud computing environment must first be classified by the appropriate Information Owner.
- A cloud services responsibility model must be established, and responsibilities for both the cloud service provider and GOS, acting as the cloud service customer, must be documented and well understood by all stakeholders.
- Security controls must be applied based on the information classification. Detailed requirements are specified in Information Protection Security Controls (IPSC) for classified data.
- All GOS data with Personally Identifiable Information (PII) must be stored in Canada.
- All GOS data with PII must be encrypted during transit and at rest.
- Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.
- No subnet containing classified data can be directly accessed over the public internet or across datacenters. Access to those subnets must be routed through intermediate subnets.
- GOS mitigation mechanisms must be in place for all publicly accessible network endpoints (e.g. public-facing websites).
- All connections between managed networks (either on-premises or cloud) must use a modern secure protocol.
- Automated monitoring systems must audit and enforce governance and security configuration requirements and capture relevant log data needed to evaluate security-related risks.
- All code development must adhere to established secure coding guidelines to mitigate against security vulnerabilities and ensure the integrity of applications and systems.
- All applications developed, acquired, or utilized by the organization must adhere to established application security standards and guidelines to mitigate against security threats and vulnerabilities.
- Zero trust principles – never trust, always verify; assume breach; least privilege – must be enforced for all users, devices, applications and data.
- Business continuity and disaster recovery plan must be in place and tested on a regular basis.
- Suppliers and contractors delivering or maintaining cloud services to Government of Saskatchewan must meet or exceed GOS security requirements.

Supporting Internal Resources

Resource	Description
Internal Security Governance Policy	All GOS 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 GOS.

Disposal of Electronic Storage Devices	This document defines the requirements around electronic storage devices.
GOS Acceptable Use Policy	This document mandates that GOS assets to be used in a responsible way.

Non-Compliance

In cases where it is determined that a breach or violation of GOS 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.

Definitions

Information Asset: An information asset refers to anything valuable to Government of Saskatchewan that should be protected from unauthorized access, use, discloser, modification, destruction, or compromise. This definition includes not only tangible items, such as hardware, software, and network equipment, but also intangible assets, which incorporate other elements, such as information, knowledge, intellectual property, and reputation.

Revision History

Version ID	Date of Change	Author	Rationale
V1.0	22 May 2025	CSRM	First Draft