

# Supplier Relationships Security Policy

Ministry of SaskBuilds and Procurement

Information Technology Division, Cyber Security and Risk Management Branch

## Supplier Relationships Security Policy

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

Last revised: October 2023

Last reviewed: October 2023

**Next review: October 2024**

# Supplier Relationships Security Policy

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

## Contents

PURPOSE..... ERROR! BOOKMARK NOT DEFINED.

SCOPE ..... 2

GOVERNING LAWS, REGULATIONS, AND STANDARDS..... 2

POLICY STATEMENTS..... 3

SUPPORTING INTERNAL RESOURCES..... 3

NON-COMPLIANCE ..... 3

EXCEPTIONS ..... 4

DEFINITIONS ..... 4

REVISION HISTORY ..... 4



# Supplier Relationships Security Policy

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

## Purpose

To ensure proper protection of the Government of Saskatchewan assets that are accessed by suppliers, and to maintain an agreed level of information security in supplier agreements.

## Scope

This Supplier Relationships 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	<a href="#">P-21.pdf (justice.gc.ca) Government of Canada Privacy Act</a>
PIPEDA	<a href="#">P-8.6.pdf (justice.gc.ca) Government of Canada PIPEDA Act</a>
Freedom of Information and Protection of Privacy Act	<a href="#">Saskatchewan's provincial public sector privacy law</a>
Local Authority Freedom of Information and Protection of Privacy Act	<a href="#">Saskatchewan's municipal public sector privacy law</a>
Health Information Protection Act	<a href="#">Saskatchewan's privacy law relating to health records</a>
ISO/IEC 27001:2013	15.1.1, 15.1.2, 15.1.3, 15.2.1, 15.2.2
ISO/IEC 27002:2022	5.19-22
NIST (National Institute of Standards and Technology) SP 800-53 v4	SR-1~7, SR-9

# Supplier Relationships Security Policy

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

## Policy Statements

- Procedures surrounding risk mitigation of a supplier’s access to The Government of Saskatchewan’s assets must be documented, reviewed, and agreed upon by The Government of Saskatchewan and the specific supplier.
- All suppliers that access, process, store, or provide various IT components must agree with The Government of Saskatchewan’s security requirements around suppliers’ relationships with the assets.
- Security requirement agreements for suppliers must also include details on addressing risks surrounding the handling, processing, and communicating of assets or services.
- Government of Saskatchewan must regularly review, validate, and update agreements with external parties to ensure they are still required and fit for purpose with relevant information security clauses.
- Process surrounding audit of supplier’s environment by Government of Saskatchewan, or a 3<sup>rd</sup> party auditor must be documented, reviewed, and agreed upon by The Government of Saskatchewan and the specific supplier.

## 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
Overarching Security Policy	Provides a framework to manage information security for all Government of Saskatchewan (GoS) information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and information users.

## 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

# Supplier Relationships Security Policy

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

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.

## Revision History

Version ID	Date of Change	Author	Rationale
V1.0	October 23, 2023	CSRM	First Draft
V1.2	November 22, 2023	CSRM	Final Draft