Asset Management 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

Asset Management Policy

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

Contents

Asset Management Policy

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

Purpose

The purpose of this policy is to ensure assets are identified appropriately and the proper protection controls in accordance with their sensitivity and value to The Government of Saskatchewan. Individuals need to understand the responsibility way of using GoS assets. This policy defines governing regulations, internal and industry standards required to access Government of Saskatchewan assets.

Scope

This Asset Management 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	8.1.1-8.1.4, 8.2.1-8.23,8.3.1-8.3.3
ISO/IEC 27002:2022	5.1, 5.9, 5.10, 5.11, 5.12, 5.13, 7.10
NIST (National Institute of Standards and Technology) SP 800-53 v4	PE-20, 16, CM-8, PS-4,5, RA-2, MP-2~7
NIST SP 800-171	3.7, 3.8, 3.3

Policy Statements

- An inventory of information assets, including owners, must be developed, and maintained.
- Rules for the acceptable use of information assets must be identified, documented, and implemented.
- Personnel and other interested parties as appropriate must return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement.
- Information must be classified and labelled according to legal requirements, value to the organization, their criticality to the organization, and sensitivity if they were to be disclosed by an unauthorized party.
- Storage media must be managed through life cycle of acquisition, use, transportation, and disposal and must be in compliance with GoS Electronic Storage Media Disposal Policy.

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
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 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

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
V1.01	19 September 2023	CSRM	First Draft
V1.2	12 November 2020	CSRM	Final Draft