Access Control 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

Access Control Security Policy

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

Contents

Access Control Security Policy

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

Purpose

The purpose of this policy is to ensure users and applications have the appropriate access levels specifically authorized to them to access information systems. Individuals need to understand the responsibility their access level provides them. This policy defines governing regulations, internal and industry standards required to access Government of Saskatchewan assets.

Scope

This Access Control 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	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)
ISO/IEC 27002:2022	5.15, 5.16, 5.17, 5.18
NIST (National Institute of Standards and Technology) SP 800-53 v4	AC-1~AC-25
NIST SP 800-171	3.1.1-3.1.22

Access Control Security Policy

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

Policy Statements

- The Government of Saskatchewan must limit physical and logical access for information systems to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- The Government of Saskatchewan must limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- The Government of Saskatchewan must ensure that authentication requirements are defined based on risk for users, processes, and devices.
- The Government of Saskatchewan must have specific access controls based on the classification of the data that is being managed.
- All user access must conform to internal policies and standards as listed in the supporting internal resources table.
- All access to systems via API, machine to machine or other interface mechanisms must conform to the internal policies and standard as listed in the supporting internal resources table.

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
Cryptography Policy/Standard	This document defines the required cryptography standards that are required the Government of Saskatchewan assets
Wireless Access Standard	This document defines the required controls that are required to deliver access to the Government of Saskatchewan Wireless Networks
Remote Access Standard	This document defines the required controls that are required to deliver access to the Government of Saskatchewan remote access
Mobility Standard	This document defines the required control that in place for Mobility devices within the Government of Saskatchewan

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

This section intentionally left blank.

Revision History

Version ID	Date of Change	Author	Rationale
V1.1	Feb 21, 2023	CSRM	Updated removing standards and specifications, referencing external documents
V1.2	October 24, 2023	CSRM	Updated for changes review