Communications and Network Security Policy

Ministry of SaskBuilds and Procurement
Information Technology Division (ITD)
Cyber Security and Risk Management Branch (CSRM)

Last revised: May 2023
Last reviewed: October 2023
Next review: October 2024

Communications and Network Security Policy

Ministry of Sask Builds and Procurement
Information Technology Division,
Cyber Security & Risk Management Branch

Contents

Communications and Network Security Policy

Ministry of Sask Builds and Procurement
Information Technology Division,
Cyber Security & Risk Management Branch

Purpose

The purpose of this policy is to ensure users, applications and infrastructure have the appropriate communications and network security levels specifically authorized for use. Individuals need to understand their responsibility in order to adhere to the Government of Saskatchewan policies as it pertains to communications provided to internal and external government agencies and ministries. This policy outlines the need for proper controls, services, and network isolation, for systems and applications. This policy defines governing regulations, internal and industry standards required to access Government of Saskatchewan assets.

Scope

This Communications and Network 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	*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.13, A.13.1, A.13.2
ISO/IEC 27002:2022	5.14, 6.6, 8.20, 8.21,8.22
NIST (National Institute of Standards and Technology) SP 800-53 v4	XX-1 control, SA-5, CM-2~CM-9, AC-5, SA-9, SA-10, AU-4, AU-5, CP-2, SA-2, SC-5, CA-2, CA-6, SA-4, SA-11, AC-19, AT-2, AT-3, IR-2, IR-8, MA-3, MP-7, SC-42, SI-1, SI-3, SI-5, SI-7, SA-8, SC-2, SC-3, SC-7, SC-18, CP-9, AC-3, AC-17, AC-18, AC-20, SC-8, SC-15, CA-3, MP-5, AU-10, IA-2, IA-8, SC-7, SC-8, SC-13, AC-3, AC-22, SI-4, SI-7, SI-10, AU-2, AU-3, AU-8, AU-11, AU-

	12, AU-14, AU-6, AU-7, AU-12, CM-6, CM-11, PE-6, PE-8, SC-7, SI-4, SI-6, SI-7,
NIST SP 800-171	

Policy Statements

- The Government of Saskatchewan must have rules, procedures, and agreements to protect information in transit to reflect the classification of the information involved.
- The Government of Saskatchewan communication's policy must be applied to Information transfer through electronic, physical storage media and verbal transfer.
- The Government of Saskatchewan must maintain confidentiality or non-disclosure agreements to address the requirement to protect confidential information using legally enforceable terms.
- The Government of Saskatchewan must maintain networks and network devices that are secured, managed, and controlled to protect information in systems and applications.
- The Government of Saskatchewan must maintain security mechanisms, service levels and service requirements for network services and be identified, implemented, and monitored.
- The Government of Saskatchewan must establish the use of logical groups of information services, users and information systems must be segregated in the organization's networks.

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
Communications and Network Security Standard	This document defines the required controls that are in place for all communications and network standards for 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
V1.0	May 27,2023	CSRM	Updated removing standards and specifications, referencing external documents
V1.2	October 25, 2023	CSRM	Final Review