System Acquisition, Development and Maintenance Security Policy

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

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

This document is intended for the Saskatchewan Ministry of SaskBuilds and Procurement, Information Technology Division, and partner organizations. It may contain legally privileged and/or confidential information and must not be disseminated, distributed, or copied

System Acquisition, Development and Maintenance Security Policy

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

Contents

System Acquisition, Development and Maintenance Security Policy

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

Purpose

The purpose of this policy is to address the operational lifecycle of system acquisition, development, and maintenance processes to have the appropriate security controls applied throughout any system project or program across their entire lifecycle. 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 System Acquisition, Development, and Maintenance Policy applies to all programs and projects that are being delivered to the Government of Saskatchewan to ensure that all informational risks are effectively addressed.

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.14.1, A.14.2, A14.3
ISO/IEC 27002:2022	5.8, 8.25, 8.26, 8.27, 8.29, 8.30, 8.31, 8.32, 8.33
NIST (National Institute of Standards and Technology) SP 800-53 v4	PL-7, PL-8, RA-2, SA-1~SA-5, SA-8, SI-10, SI-6, SI-7, SI-10, AU-10, SC-8, SC-23, SI-7, SI-15, AC-1, MP-1, SC-1, SC-12, SC-17, CM-1~CM-11, SC-18, S1-7, AC-3, AC-6, CM-5, CM-9, MA-5, SA-10, CM-1, CM-3, CM-9, SA-10, CM-4, CM-5, AC-4, AU-13, PE-19, SC-31, SC-38, SA-9, SA-12, SA-13, SA-15, CA-7, RA-3, RA-5, SI-2, SI-5

NIST SP 800-171	3.16; - 3.16.1; 3.16.2; 3.16.3

Policy Statements

- The Government of Saskatchewan must maintain the confidentiality, integrity, and availability of the information across the entire lifecycle of a program and/or project based on the data classification identified by the Statement of Sensitivity (SoS) form.
- The Government of Saskatchewan must ensure that security be an integral part of all programs and/or projects.
- The Government of Saskatchewan must ensure that all security requirements are identified and addressed when developing or acquiring systems and incorporated in the procurement process.
- All programs and/or projects must ensure that they meet or exceed the current defined principles, policies, standards, and controls for developing, maintaining, and operating information systems for the Government of Saskatchewan. This extends to outsourced development and operations that are being performed by outside agencies.
- The Government of Saskatchewan must maintain both production and non-production environments while delivering information systems. These environments all require the appropriate level of controls based on the classification and risk of the information that may be exposed.
- The Government of Saskatchewan must ensure that the data in the non-production environments do not contain sensitive information.
- To maintain compliance all non-production environments must use the appropriate information to validate their test scenarios. Sensitive production data must not be used in non-production environments without masking, obfuscation, or de-identification.
- The Government of Saskatchewan must ensure that all development source code be managed according to the standards and technologies as defined in the System Acquisition, Development and Maintenance Security Standard.
- The Government of Saskatchewan must perform the required level testing to validate functionality and mitigate any identified risks within the systems prior to deployment to any production environment using the established change management and communication practices.

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
Statement of Sensitivity	This document evaluates the data within a project to determine the appropriate class of data and identifies which controls will need to be applied in accordance with the IPSC document.
System Acquisition, Development, and Maintenance Security Standard	This standard document provides guidance as to the standards and appropriate use of environments, data, and controls required as part of programs and/or project life cycles.

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.

System Acquisition, Development and Maintenance Security Policy

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

Definitions

This section intentionally left blank.

Revision History

Version ID	Date of Change	Author	Rationale
V1.1	23 June 2023	CSRM	Updated to new format removing of standards and specifications, referencing external documents
V1.2	25 October	CSRM	Final Review