Compliance Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Information Security Branch

Last revised: April 2021
Last reviewed: April 2021
Next review: April 2022

Purpose

The purpose of this policy is to ensure proper measures are in place to avoid non-adherence to information security compliance requirements – legal, contractual, regulatory, or otherwise.

Scope

This Compliance Policy applies to all business processes and data, information systems and components, personnel, and physical areas of The Government of Saskatchewan. All employees and contractors must comply with all policies, standards, and contractual requirements that govern the use of the intellectual property and proprietary software products.

Definitions

This section intentionally left blank.

Governing Laws & Regulations & Standards

Guidance	Section
ISO27001:2013	A.18 (A.18.1, A.18.2)
NIST SP 800-53 v4	XX-1 controls, CM-10, AC-3, AU-9, AU-11, CP-9, MP-4, SA-5, SI-12, Appendix J Privacy Controls, SI-12, AC-8, AU-6, CM-11, PL-4, PS-6, PS-8, IA-7, SC-13, CA-2, CA-7, RA-5, AU-1, AU-2, SI-4

Policy Statements

Compliance with legal and contractual requirements:

- To avoid breaches of legal, statutory regulatory or contractual obligations related to information security, the statutory, regulatory, and contractual requirements shall be:
    - Identified, documented, and well-maintained.
    - Any intellectual property rights requirements should be implemented and adhered to, as necessary.
    - Records will be properly managed to avoid any destruction from natural disasters, unauthorized use, or loss.
    - Personally, Identifiable Information (PII) will be properly protected.
    - Any cryptographic controls will be used appropriately according to relevant compliance requirements.
- *The Archives and Public Management Act, 2015*, subsidiary regulations and policies outline the requirements for the retention and disposal of government records.
- The Provincial Archives of Saskatchewan are responsible for:
    - Providing records and information management service to the Provincial Government
    - The development and dissemination of policies, procedures, standards, and guidelines related to records and information management
    - Records management advice and support to government institutions
    - Processing the requests for disposal of government records

- *The Saskatchewan Records Management Policy* is published on the Provincial Archives of Saskatchewan's website.

- Security controls must be applied to protect the privacy and personally identifiable information following the relevant legislation.
  - *The Freedom of Information and Protection and Privacy Act*, its subsidiary Regulations and policies govern the protection of personal information held by the Government of Saskatchewan.
  - The Ministry of Justice's *Access and Privacy Branch* helps government institutions in their compliance with this legislation.

Compliance with security policies and standards:

- At least annually, The Government of Saskatchewan should perform independent reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.
- Results from compliance reviews or audits shall be documented and reported by The Government of Saskatchewan's leadership.
- The Chief Information Officer may initiate a supplemental audit or review to:
  - Assess the effectiveness of the Information Security Program
  - Document the results
  - Report the results to senior management
- The Chief Information Officer must address the weaknesses and non-compliant controls that are identified in reports from the Provincial Auditor or independent reviewers.

Information system audit considerations:

- The Government of Saskatchewan should implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.
- The Government of Saskatchewan shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.
- The Government of Saskatchewan's information systems should be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.
- The Government of Saskatchewan should report findings of audit records reviews to information security personnel and Information Security Branch leadership.

Information security reviews and continuous improvements:

- The Government of Saskatchewan will conduct an independent review of its information security practices, controls, policies, etc.
- The management team is responsible for regular reviews of their compliance with information security policies and procedures.
- A technical review of information systems will be conducted regularly.
- The Government of Saskatchewan should develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified because of internal/external risk assessments, security reviews, and/or audits.

- Information Owners and Service Owners must ensure security standards, policies and processes are implemented and adhered to by:
    - Conducting periodic self-assessments
    - Initiating independent assessments, review, or audits
    - Ensuring personnel receive regular information security awareness updates
- When the review process indicates non-compliance with standards or policies, Information Owners and Service Owners must:
    - Determine the cause(s)
    - Assess the threats and risks associated with non-compliance
    - Document the risks
    - Determine and implement corrective actions to take

Relevant Procedures

This section intentionally left blank.

Non-Compliance

In cases where it is determined that a breach or violation of Government of Saskatchewan policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, 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 acceptable of risk by the Security Governance Committee. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Branch. Policy exceptions will be reviewed periodically for appropriateness.

Revision History

Version ID	Date of Change	Author	Rationale