Security Compliance Policy

Information Security Branch, Ministry of Central Services

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

This document outlines Government of Saskatchewan Security Compliance Policy.

Purpose

To comply with all relevant legal, statutory, regulatory, and contractual information security obligations and requirements; and to ensure that information security is implemented and operated in accordance with organizational policies and procedures.

Scope

This policy applies to all GoS owned or operated information systems, intellectual property, and government records. All employees and contractors must comply with all policies, standards, and contractual requirements that govern the use of intellectual property and proprietary software products.

Policy Statements

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security, the statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained. A description of how compliance is achieved is to be kept with these records.

Controls must be implemented to ensure compliance with legal, regulatory and contractual requirements related to intellectual property rights and proprietary software licensing.

Government records must be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

- **The Archives and Public Records Management Act, 2015**, subsidiary Regulations and policies outline the requirements for the retention and disposal of government records.
- **The Provincial Archives of Saskatchewan** is responsible for:
    - providing records and information management services 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; and
    - processing the requests for disposal of government records.
    - The **Saskatchewan Records Management Policy** is published on the Provincial Archives of Saskatchewan web site.

Security controls must be applied to protect privacy and personally identifiable information in accordance with relevant legislation.

- The **Freedom of Information and Protection of 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.

Independent reviews of the Information Security Program must be regularly conducted.

- The Information Technology Division Security Program is audited annually by the Provincial Auditor of Saskatchewan.
- The Chief Information Security Officer may initiate a supplemental audit or review to:
    - assess the effectiveness of the Information Security Program;
    - document the results; and
    - report the results to senior management.
- This review must be conducted by an independent supplier.
- The Chief Information Security Officer must address the weaknesses and non-compliant controls that are identified in reports from the Provincial Auditor or independent reviewers.

Managers must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.

- 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, reviews or audits; and
    - ensuring personnel receive regular information security awareness updates.
- When review processes indicate non-compliance with standards or policies, Information Owners and Service Owners must:
    - determine cause(s);
    - assess the threats and risks on non-compliant processes;
    - document the marginal risks; and
    - determine and implement corrective action.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS 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 on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.