Security Policy Management Directive

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

Information Security Branch, Ministry of Central Services

This document outlines the Security Policy Management Directive at the Government of Saskatchewan.

Purpose

To provide management direction and support for information security in accordance with the government's business requirements and relevant laws and regulations.

Scope

This policy applies to all GoS owned or operated information systems, intellectual property, and government records.

Policy Statements

Issuance of Policies and Standards

The Chief Information Security Officer is responsible for establishing, issuing and monitoring the compliance of information security standards and policies.

The Information Security Policies and Standards contain operational policies and standards intended to safeguard the confidentiality, integrity and availability of government information and information systems. They establish the minimum requirements for the secure delivery of government services through:

- management and business processes that include and enable security processes;
- ongoing security awareness for personnel;
- physical security for sensitive information assets;
- governance processes for information technology;
- reporting of information security incidents;
- including information security in business continuity planning; and
- monitoring for compliance.

Review of Policies and Standards

The Chief Information Security Officer must, at least every two years, ensure that the information security policies, standards, specifications and guidelines are reviewed in an effort to ensure their continuing adequacy and effectiveness. Reviews must consider:

- feedback from stakeholders;
- legislative, regulatory or policy changes that impact information security and/or information management;
- the planning and implementation of new or significantly changed technology;
- major initiatives (e.g. new information systems or contracting arrangements);
- audit reports or reviews of security controls that identify high risk vulnerabilities;
- threat or vulnerability trends produced from automated monitoring processes that indicate an increased risk to information assets;
- reports from security incident investigations;
- the renewal of supplier access agreements which involve major government programs or services;

- the introduction or revision of national, international or industry standards for information security that address emerging technology issues; and
- reports from associated external agencies (e.g. Privacy Commissioner, Police) that identify emerging trends related to information security.

Security is a Process

The Chief Information Security Officer (CISO) recognizes that information security is a process. In order to be effective, it requires management commitment and continuing security awareness efforts. Other principles that guide the government's directions are:

- information security requires a multi-layered defense strategy, and
- security is everyone's responsibility.

Ministry-specific Policies and Standards

The Information Security Standards establish a baseline level of security that applies throughout government. Ministries may develop and implement additional policies, standards and guidelines for use within their organization or for a specific information system or program. Those additional policies may exceed but must not conflict with these standards.

Ministries must provide the Chief Information Security Officer with copies of any locally developed information security policies, standards or guidelines.

The Chief Information Security Officer must maintain a central repository for the collection of Ministry-developed policies, standards or guidelines.

Where Ministries have developed specific standards and policies, they must review them at least every two years and provide the Chief Information Security Officer with updated versions.

Risk Management Decision Item

When information security policies or standards cannot be complied with, the details must be documented in a Risk Management Decision Item (RMDI). The RMDI must record the standards or policies violated and the risks associated with the non-compliance.

When the request involves a Ministry application or system, the risks must be accepted by the Ministry Security Officer. When the issue involves Information Technology Division only, the Manager, Information Security Branch (acting on behalf of the CISO), must sign and accept the risk before the non-compliant request is implemented.

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. Policy exceptions will be reviewed on a periodic basis for appropriateness.