Information Security Incident Management Policy

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

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security policy for Information Security Incident Management.

Purpose

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Scope

This policy applies to the management of all Government of Saskatchewan information security events and incidents.

Policy Statements

Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.

The Executive Director, Information Security Branch, is responsible to ensure the following procedures are developed and implemented:

- incident response planning and preparation;
- monitoring, detecting, analyzing and reporting of information security events and incidents;
- logging incident management activities;
- handling of forensic evidence;
- assessment of and decision on information security events and assessment of information security weaknesses; and
- response and recovery from an incident.

All users of Government information systems must report information security events immediately to the Information Technology Division Service Desk. Examples of events include, but are not limited to:

- ineffective security control;
- breach of information confidentiality, integrity or availability expectations;
- human errors;
- non-compliance with standards, policies or guidelines;
- breaches of physical security;
- uncontrolled system changes;
- unauthorized installation of software or hardware;
- malfunctions of software or hardware;
- access violations;
- malicious software; and
- lost or stolen information assets.

Information security events reported to a Ministry by a supplier must be further reported to Information Security Branch.

All users of Government information systems must note and report any observed or suspected security weaknesses to their Ministry Security Officer. No user may attempt to exploit any security weakness.

Information Security Branch must assess each information security event. Based on the incident classification scale it must be decided if the event must be classified as an information security incident. Results of the assessment and decision must be recorded in detail for future reference and verification.

Information security incidents must be responded to by Information Security Branch personnel or others designated by the Executive Director, Information Security Branch, using documented procedures. The response procedures must include:

- collecting evidence as soon as possible after the occurrence;
- conducting information security forensics analysis if required;
- escalation, if required;
- ensuring that all response activities are properly logged for later analysis;
- communicating the existence of the incident and any relevant details to internal and external people and organizations with a “need-to-know;”
- dealing with information security weaknesses found to have caused or contributed to the incident; and
- once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis must take place, as necessary, to identify the source of the incident.

Service Owners must ensure that incidents involving supplier services are handled in accordance with the procedures documented in supplier agreements.

Information Security Branch is responsible for monitoring and evaluating information security incidents in order to reduce the likelihood or impact of future incidents by:

- using statistical analysis of incident frequency, type and location to identify trends;
- ensuring incident reports and trends are used to promote continuous improvement of security standards, policies and processes, security awareness and training programs, and Business Continuity and Disaster Recovery Plans;
- advising Information Owners and Ministry Security Officers of evolving security threats and mitigation strategies;
- evaluating the effectiveness of incident management, response and reporting; and
- evaluating the effectiveness of information security technologies.

Evidence collected during information security incident investigations must be collected using processes developed by the Information Security Branch that ensures it can be reliably used for legal or disciplinary proceedings (in the event that such proceedings occur) in an effort to help ensure the admissibility and weight.

At minimum:

- The chain of custody must be maintained;
- Evidence may only be collected by individuals authorized by the Chief Information Security Officer;
- For evidence on computer media:
    - mirror images or copies must be made depending on the type of media;
    - a log of all actions taken during the copying process must be kept and the process witnessed;
    - the original media must be placed in a tamperproof bag, initialed and dated, kept under lock and key and remain untouched; and
    - any forensic work must only be performed on the copies of the evidential material.

Information Owners, Ministries and Agencies in receipt of a legal order to produce electronic evidence must immediately contact the Chief Information Security Officer.

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.