Security Incident Management Policy

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

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

Purpose

The purpose of this policy is to ensure proper recognition, management, and communication of security events and weaknesses through a formal process.

The quality and integrity of The Government of Saskatchewan's incident response capabilities are used to monitor for security incidents, determine the magnitude of the threat presented by these incidents, and respond to these incidents. Without an incident response capability, the potential exists that if a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected sooner.

Scope

This Security Incident Management Policy applies to all business processes and data, information systems and components, personnel, and physical areas of The Government of Saskatchewan.

Definitions

This section intentionally left blank.

Governing Laws & Regulations & Standards

Guidance	Section
ISO27001:2013	A.16.1
NIST SP 800-53 v4	AU-6, IR-1, IR-6, CA-2, CA-7, PL-4, SA-5, SA-11, SI-2, SI-5, IR-4, IR-10, AU-7, AU-8, AU-9, AU-11
GDPR	Arts. 33 & 34

Policy Statements

Management of Information Security Incidents and Improvements

- Incident management responsibilities and procedures are established to ensure timely response to incidents.
- An incident response team is established to handle the intake, communication, and remediation of security incidents. Government of Saskatchewan IT staff taking on the role of responding to incidents when required will be referred to as "incident responders".
    - Incident responders must provide primary and secondary contact information so that they can be reached in the event of a relevant security incident.
    - Incident responders will establish a method of communication alternative to the primary method that is to be used if the primary communication method is affected by or is otherwise unavailable during, the security incident [e.g., alternate non-organizational email or instant messaging platform].
    - Communication with affected parties will be provided on an as-needed basis, until the incident is contained. It is up to the discretion of the incident responders to withhold information if the disclosure of said information deems a reasonable risk to The Government of Saskatchewan's security while the response is ongoing.
- The incident response capability includes a defined plan and addresses the seven stages of incident response:
    - Preparation

    - Detection
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
- Information security events must be reported through proper channels. Incidents will be tracked as they occur within Service Now
    - Any weaknesses suspected or verified in systems and services must be reported by users (employees or third-party contractors) using those systems and services. Users should immediately contact the IT service desk.
- As information security events are assessed, determinations are made about whether they can be identified as information security incidents. Once an event is deemed a true security incident, the incident will be classified as such and relevant incident responders will be notified.
- Information security incidents will be identified and classified into different severity levels to make the incident response process more effective.
- Incidents will be responded to with the appropriate procedures based on documented organizational processes.
    - Incident response procedures will be reviewed on annual basis. Any required updates will be communicated to the appropriate parties.
- Definitions and procedures around the identification, collection, acquisition, and preservation of evidence will be established.
    - This data will be recorded and stored in a repository dedicated to Incident Management
    - The records of this data will be audited regularly and timestamped.
- In the event of a major incident, only a designated spokesperson will address the media.
- After all relevant security incidents, a post-incident review will be conducted by incident responders to determine the root cause of the incident, the consequences, and the lessons learned. The information gained from responding to and resolving incidents will be used to reduce potential future incidents. Any affected parties, including end-users, may be contacted for additional insight.

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 acceptance 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