Security Incident Management Policy

Ministry of SaskBuilds and Procurement
Information Technology Division
Cyber Security and Risk Management Branch

Last revised: October 2023
Last reviewed: November 2023
Next review: November 2024

Security Incident Management Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Contents

Security Incident Management Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Purpose

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

Scope

This Operations Security Policy applies to all business processes and data, information systems, components, personnel, and physical areas of the Government of Saskatchewan. Person(s) this policy applies to include but are not limited to:

- All employees, whether employed on a full-time or part-time basis by the Government of Saskatchewan
- Contractors and Service Providers that access and manage Government of Saskatchewan assets.

Governing Laws, Regulations, and Standards

Resource	Description
Privacy Act	*P-21.pdf (justice.gc.ca) Government of Canada Privacy Act*
PIPEDA	*P-8.6.pdf (justice.gc.ca)Government of Canada PIPEDA Act*
Freedom of Information and Protection of Privacy Act	Saskatchewan's provincial public sector privacy law
Local Authority Freedom of Information and Protection of Privacy Act	*Saskatchewan's municipal public sector privacy law*
Health Information Protection Act	*Saskatchewan's privacy law relating to health records*
ISO/IEC 27001:2013	16.1
ISO/IEC 27002:2022	5.24~28, 6.8
NIST (National Institute of Standards and Technology) 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

Security Incident Management Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Policy Statements

- Incident management responsibilities and procedures must be established to ensure timely response to security incidents.
- An incident response team must be established to handle the intake, communication, and remediation of security incidents. 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 incidents must be documented and tracked as per a defined plan and addresses the seven stages of incident response:
    - Preparation
    - Detections
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
- Information security events must be reported through proper channels. Incidents must be tracked as the occur in a secure enterprise grade platform.
    - 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 based on impact to the Government of Saskatchewan and relevant incident responders will be notified.
- Incidents will be addressed with the appropriate incident response procedures
    - 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 or department 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.

Supporting Internal Resources

Resource	Description
Internal Security Governance Policy	All Government of Saskatchewan Security Policies align to this Governance Policy
Information Protection Security Controls (IPSC) for Classified Data	This document defines the required access controls required to provide the proper security based on Classified Data for Government of Saskatchewan
GoS Incident Response Plan	Documented procedures, contact information and playbooks.

Non-Compliance

A breach of this policy may lead to discipline, up to and including termination, in accordance with PS 803 Corrective Discipline policy. Similarly, for contracted resources or entities, Government of Saskatchewan will initiate corrective measures up to and including restricting access to services or initiating disciplinary action up to and including termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In cases where it is determined that a breach or violation of Government of Saskatchewan Information Security policies has occurred, the respective Ministry under the direction of the Chief Information Officer and Information Security Branch, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, in accordance with PS 803 Corrective Discipline policy, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Definitions

This section intentionally left blank.

Revision History

Version ID	Date of Change	Author	Rationale
V1.0	October 20, 2023	CSRM	First Draft
V1.2	November 23, 2023	CSRM	Final Draft