Business Continuity Planning Security 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

Business Continuity Planning Security Policy

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

Contents

Business Continuity Planning Security Policy

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

Purpose

The purpose of this policy is to ensure that information security is properly addressed within the organization's Business Continuity Planning (BCP) strategy.

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	17.1~17.3
ISO/IEC 27002:2022	5.29, 8 .14
NIST (National Institute of Standards and Technology) SP 800-53 v4	CP-1, CP-2, CP-4, PM-9, RA-3, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13

Policy Statements

- The Government of Saskatchewan should determine its requirements for adapting information security controls during disruption. Information security requirements should be included in the business continuity plan (BCP)
- The Government of Saskatchewan should establish a process to ensure that the security requirements listed in BCP are reviewed and approved by senior management.
- The Government of Saskatchewan should conduct a Business Impact Analysis (BIA) to identify security functions, processes, and applications that are critical to The Government of Saskatchewan and determine a point in time (i.e., recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to the Government of Saskatchewan.
- The Government of Saskatchewan should utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical security functions, processes, and applications.
- The Government of Saskatchewan should assign contingency roles and responsibilities to key individuals from all security functions.
- The Government of Saskatchewan should establish procedures to maintain continuity of critical security functions despite critical information system disruption, breach, or failure.
- The Government of Saskatchewan should distribute copies of the BCP to key personnel responsible for the recovery of the critical security functions and other relevant personnel and partners with contingency roles, as determined by information owners and service owners.
- Information Owners and Service Owners must identify business requirements for the availability of information systems. Information System must be implemented with redundancy sufficient to meet availability requirements. When the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.

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
Operations Security Policy	Ensures correct and secure operations of information systems, and that the impact of change activities on operational systems are minimized.

Non-Compliance

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.

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 Security Officer, under the guidance of the Cyber Security and Risk Management Branch. Policy exceptions will be reviewed periodically for appropriateness.

Definitions

This section intentionally left blank.

Revision History

Version ID	Date of Change	Author	Rationale
V1.0	20 October 2023	CSRM	First Draft
V1.2	12 November 2023	CSRM	Final Draft