Information Security Aspects of Business Continuity Planning 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 that information security is properly addressed within the organization's Business Continuity Planning (BCP) strategy.

Scope

This Information Security Aspects of Business Continuity Planning 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.17 (A.17.1, A.17.2)
NIST 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

Information Security Continuity Management:

- The organization will determine its requirements for information security and how it fits into the overall continuity of information security management in crises.
    - Including aspects like purpose, roles, and responsibilities.
- The organization will create, document, and implement any processes and controls related to the continuity of information security during crises.
    - Contingency plans will go through testing to ensure comprehensiveness and effectiveness.
- These information security processes and controls will be reviewed and validated regularly to ensure their continued effectiveness.

Security Contingency Planning within the context of enterprise BCP:

- 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 document a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable The Government of Saskatchewan to respond to potential disruptions and recover its critical security functions within a predetermined RTO following a disruption.
- The Government of Saskatchewan should establish a process to ensure that the BCP is reviewed and approved by senior management.
- 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 The Government of Saskatchewan

Redundancies:

- Sufficient redundancies will be implemented to ensure availability requirements are met.
- Information System must be implemented with redundancy sufficient to meet availability requirements
- Information Owners and Service Owners must identify business requirements for the availability of information systems. When the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.

Data Backups:

- The Government of Saskatchewan should develop, maintain, and document data backup and storage procedures to ensure the recovery of electronic information in the event of failure.
- The Government of Saskatchewan should identify and apply security requirements for protecting data backups based on the different types of data (sensitive, confidential, public) handled by the entity.
- The Government of Saskatchewan should establish a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.

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 acceptable 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
