Security Aspects of Business Continuity

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

Information Security Branch, Ministry of Central Services

This document outlines Government of Saskatchewan security policy for Business Continuity.

Purpose

To embed information security continuity in the government's business continuity management systems and to ensure availability of the government's information systems.

Scope

This policy applies to all GoS owned or operated information systems, assets, and operations.

Policy Statements

Information Security Continuity

The government must determine its requirements for information security and the continuity of information security management in a crisis, disaster or other adverse situations:

- Information security requirements must be determined when planning for business continuity and disaster recovery;
- Information Owners and Service Owners must determine whether the continuity of information security is captured within the business continuity management process and the disaster recovery management process; and
- In the absence of formal business continuity and disaster recovery planning, information security management must assume that information security requirements remain the same in adverse situations, compared to normal operational conditions.

The government must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. Information Owners and Service Owners must ensure that:

- an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
- incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated; and
- documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event while maintaining its information security to a predetermined level based on management-approved information security continuity objectives.

Information Owners and Service Owners must establish, document, implement and maintain:

- information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- process, procedures and implementation changes to maintain existing information security controls during an adverse situation; and
- compensating controls for information security controls that cannot be maintained during an adverse situation.

The government must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. Information Owners and Service Owners must verify information security management continuity of its information assets by:

- exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;
- exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with continuity objectives; and
- reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Redundancies

Information systems 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.
- Where applicable, redundant information systems must be tested to ensure the failover from one component to another works as intended.

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.