Security in Supplier Relationships 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 protection of The Government of Saskatchewan assets that are accessed by suppliers and to maintain an agreed level of information security in like with supplier agreements.

Scope

This Security in Supplier Relationships 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.15 (A.15.1, A.15.2.)
NIST SP 800-53 v4	SA-12

Policy Statements

Information Security in Supplier Relationships:

- Procedures surrounding risk mitigation of a supplier's access to The Government of Saskatchewan's assets must be documented, reviewed, and agreed upon by The Government of Saskatchewan and the specific supplier.
- All suppliers that access, process, store, or provide various IT components must agree with The Government of Saskatchewan's security requirements around suppliers' relationships with the assets.
    - Types of information access should be defined that different types of suppliers will be allowed, as well as monitoring and controlling the access.
    - Types of obligations applicable to suppliers should be defined to protect the organization's information.
- Security requirement agreements for suppliers must also include details on addressing risks surrounding the handling, processing, and communicating of assets or services.
    - The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
    - Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, etc. should be identified and addressed.

Supplier Service Delivery Management:

- A process must be developed to monitor and assess the service delivery of a supplier to ensure it is meeting appropriate business and security requirements, as well as meeting any contract or SLA requirements.
- A change management process must be in place to address any alterations to an existing policy, including documentation of said change and ensuring it is in alignment with business processes and follows appropriate re-assessment of risk involved, if necessary.

- Non-security-related items must be handled per the Procurement Policies of the Ministry of Central Services. These processes include:
    - Designating responsibility for monitoring to an employee
    - Monitoring service performance levels to verify adherence to the agreements.
    - Reviewing service reports produced by the supplier.
    - Conducting audits of suppliers and follow-up on identified issues
    - Handling information security incidents under Information Security Incident Management and implementing any recommended controls that follow from the review.
    - Resolving and managing any other identified problems
    - Ensuring the supplier maintains sufficient service capabilities under the Security Aspects of Business Continuity Management Policy where applicable.
- Information Owners and Service Owners must ensure agreements with suppliers include provisions for amending agreements in response to changes in legislation, regulation, business requirements, standards, policies, or service delivery.
- Information Owners and Service Owners must ensure that the security-related change management process for services delivered by supplies includes:
    - Reviewing and updating the Threat and Risk Assessment (or other related security assessments) to determine the impact on security controls.
    - Implementing new or enhanced security controls when identified by the risk assessment.
    - Reviewing and updating the Privacy Impact Assessment
    - Initiating and implementing revisions to standards, policies, and procedures.

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
