Supplier Relationships Security Policy

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

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security policy pertaining to Supplier Relationships.

Purpose

To ensure protection of government information assets that are accessible by suppliers and to maintain an agreed level of information security in line with supplier agreements.

Scope

This policy applies to all Government of Saskatchewan supplier relationships.

Policy Statements

Information Security in Supplier Relationships

Information security requirements for mitigating the risks associated with suppliers' access to the government's information assets must be agreed with the supplier and documented. Security controls compliant with the Standards must be implemented before a supplier is allowed to access the government's information assets. The controls include processes and procedures to be implemented by government and those that must be implemented by the supplier.

Arrangements with suppliers that involve accessing, processing, storing, communicating or managing the Government's information, information systems or information processing facilities must be based on a formal agreement containing necessary security requirements.

Information Security Branch must define the information security requirements that apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships. At minimum, these must include requirements to address the risks associated with information and communications technology services and product supply chains.

Supplier Service Delivery Management

Information Owners and Service Owners must monitor and review the security-related terms and conditions in agreements with suppliers. Non-security related items must be handled in accordance with Procurement Policies of the Ministry of Central Services. The processes must 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 in accordance with the ***Information Security Incident Management*** and implementing any recommended controls that follow from the review;
- resolving and managing any other identified problems; and
- ensuring the supplier maintains sufficient service capability in accordance with 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 suppliers includes:

- reviewing and updating the Threat and Risk Assessment (or other related security assessment) 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 (if applicable); and
- initiating and implementing revisions to standards, policies and procedures.

Contact the Ministry of Central Services for complete procurement policies and standards.

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.