Supplier Relationships Security Standard

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 standards for Supplier Relationships.

Table of Contents

Reference Documents

The following documents are available on the IT Security Services Taskroom:

- *Supplier Relationships Security Policy*

Government of Saskatchewan

1. Information Security in Supplier Relationships

1.1. Information Security Standard for Supplier Relationships

Security controls 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. Among the controls are:

- identifying and documenting the types of suppliers (e.g. IT services, logistics, utilities, financial services, IT infrastructure) that the government will allow to access its information;
- a standardized process and lifecycle for managing supplier relationships;
- defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;
- minimum information security requirements as determined by the data classification and type of access to serve as the basis for individual supplier agreements based on the government's needs and its risk profile;
- processes and procedures for monitoring adherence to established information security requirements for suppliers and type of access, including third party review and product validation;
- accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;
- types of obligations applicable to suppliers to safeguard the government's information;
- handling incidents and contingencies associated with supplier access including responsibilities of both the government and suppliers;
- resilience, recovery (if necessary), and contingency arrangements to ensure the availability of the information or information processing provided by either party;
- awareness training for the government's personnel involved in acquisitions regarding applicable standards, policies, processes and procedures;
- awareness training for the government's personnel interacting with suppliers regarding rules of engagement and behaviour based on the type of supplier and the level of access;
- conditions under which information security requirements and controls will be documented in an agreement signed by both parties;
- managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period; and
- non-disclosure agreements to safeguard sensitive information.

1.2. Addressing Security within Supplier Agreements

Information Owners and Service Owners, in consultation with Information Security Branch, must ensure that agreements are established to document both parties' obligations to fulfil relevant information security requirements. The following terms must be considered for inclusion in the agreements:

- description of the information to be accessed and methods of access;
- the security classification level of the information and, if applicable, a mapping between the government's classification scheme and that of the supplier;
- legal and regulatory requirements, intellectual property rights and copyright requirements;

- obligation of each party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;
- rules of acceptable use;
- either 1) an explicit list of supplier personnel authorized to access or receive the government's information or 2) procedures and conditions for granting and removal of authorization for access to or receipt of the government's information by supplier personnel;
- information security standards and policies relevant to the specific contract;
- incident management requirements and procedures including notification and collaboration during incident remediation;
- training and awareness requirements;
- relevant regulations required for sub-contracting, including the controls that need to be implemented;
- a contact person for information security issues;
- screening requirements, if applicable, for supplier's personnel including responsibilities for conducting the screening and notification if screening results show cause for concern;
- right to audit the supplier's processes and controls related to the agreement;
- defect resolution and conflict resolution processes;
- supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
- supplier's obligations to comply with the government's security requirements; and
- procedures for continuing processing in the event the supplier becomes unable to supply its products or services.

1.3. Information and Communication Technology Supply Chain

Service Owners must ensure that the following are included in supplier agreements:

- for information and communication technology services, requiring that suppliers propagate the government's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to government;
- implementing a monitoring process and acceptable methods for validating that delivered products and services are adhering to the stated security requirements;
- obtaining assurance that the delivered products are functioning as expected without any unexpected or unwanted features;
- defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the government and suppliers; and
- implementing specific processes for managing information and communication technology component lifecycles and availability and associated security risks; This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.