System Acquisition, Development, and Maintenance 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 System Acquisition, Development, and Maintenance.

Purpose

To ensure that security is an integral part of information systems across their entire lifecycle, including those that provide services over public networks, that information security is integrated into the system development lifecycle, and to ensure the protection of data used for testing.

Scope

This policy applies to all Government of Saskatchewan information systems and services.

Policy Statements

Information Security Requirements Analysis and Specification

When developing, acquiring or making major changes to an information system, Information Owners and Service Owners must:

- prepare a Statement of Sensitivity to determine the confidentiality, integrity and availability requirements of the system;
- apply security controls based on a Threat and Risk Assessment;
- document the roles and responsibilities related to information system security management;
- document specific procedures and standards used to mitigate risks and safeguard the information systems; and
- document communication procedures for security-related events and incidents.

Security Application Services on Public Networks

Prior to implementing an information system that involves electronic commerce on public networks, Information Owners must ensure their protection from fraudulent activity, contract dispute, unauthorized disclosure and modification by:

- conducting an information security requirements analysis as per the previous section;
- ensure that user notification and acceptance of terms and conditions of use complies with government policies and standards; and
- ensure that multifactor authentication is used where applicable based on the data classification.

Ministries should consider including applications on public networks in their Business Continuity Planning.

Protecting Application Services Transactions

Information systems that involve on-line transactions must have security controls commensurate with the value and level of sensitivity of the information. Information Owners and Service Owners must ensure that security controls are implemented to prevent incomplete transmission, misrouting, repudiation of transactions, unauthorized message duplication and replay.

Controls to consider include:

- validating and verifying user credentials;
- digital signatures and encryption;
- secure communication protocols; and
- storing online transaction details on servers within the appropriate network security zone.

Information Owners and Service Owners must ensure that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry (PCI) Data Security Standard as published by the *PCI Security Standards Council.*

Information Owners and Service Owners must contact Information Security Branch before initiating any project that involves payment card transactions.

Secure Development

Rules for the development of software and systems must be established and applied to developments within government. Secure development is a requirement to build and support a secure service, architecture, software and system. Information Owners and Service Owners must consider:

- security of the development environment;
- guidance on security in the software development lifecycle including methodology and secure coding guidelines;
- security requirements in the design phase;
- security checkpoints within the project milestones;
- secure repositories;
- security in version control;
- required security application knowledge; and
- developers' capability for avoiding, finding and fixing vulnerabilities.

Secure programming techniques must be used for both new developments and code re-use scenarios.

System Change Control Procedures

When introducing new systems and major changes to existing systems, Information Owners and Service Owners must follow a formal change control that includes documentation, specification, testing, quality control, approval, and a managed implementation.

The change control process must also include:

- an analysis of the impacts of the change;
- specifications of security controls;
- ensuring that existing security controls are not compromised;
- ensuring that application developers can only access required program source code libraries; and
- obtaining a formal agreement and approval for the change.

The following processes must also be included:

- records of agreed authorization levels;
- change requests must be received from authorized users;
- annual reviews of change controls and integrity procedures;
- identification of all software, information, database entities and hardware that require amendment;

- accepting changes by authorized personnel prior to implementation;
- updating and archiving system, operational and user documentation;
- maintaining version control; and
- change requests logging.

Application and operational change control procedures must be integrated when practical.

New software, including patches, service packs and other updates, must be tested in an environment that is segregated from the development and production environments.

Automated updates will not be used on critical systems.

Technical Review of Applications After Operating Platform Changes
To help ensure that information systems will not be disrupted or compromised, Information Owners and Service Owners must implement the following processes:

- a technical review of application control and integrity procedures which tests the impact of operating system changes on business-critical applications;
- timely notification to allow appropriate tests and reviews before implementation; and
- assigning responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes to a specific group or individual.

Restrictions on Changes to Software Packages
A software update management process must be maintained for commercial-off-the-shelf (COTS) software. This is intended to ensure that:

- up to date and approved patches have been applied; and
- the version of software in use is supported by the vendor.

Other than patches supplied by the vendor, commercial off the shelf (COTS) software must not be modified except in extraordinary circumstances (e.g. when needed for a critical business requirement). Those circumstances must be documented and approved by the Information Owner.

If changes to COTS software are required, the Information Owner and Service Owners must determine and document:

- the impact on security controls in the software;
- the consent of the vendor, if required;
- if the required functionality is included in a newer version of the software;
- if government will be responsible for maintenance of the software after the change; and
- compatibility with other software in use.

If changes are made to COTS software the original version must be kept in an unaltered state. The changes must be:

- logged and documented, including a detailed technical description;
- applied to a copy of the original software; and
- tested and reviewed to ensure that the modified software operates as intended.

Secure System Engineering Principles

Information Owners and Service Owners must:

- ensure that secure information system engineering procedures based on security engineering principles are established, documented and applied to information system engineering activities;
- ensure that security is designed into all architecture layers: business, data, applications and technology;
- ensure the need for information security is balanced with the need for accessibility;
- analyze new technology for security risks and review the design against known attack patterns; and
- ensure that security engineering principles are reviewed and updated regularly.

Secure Development Environment

Secure development environments for system development and integration efforts must be established and appropriately protected throughout the entire system development lifecycle. The “secure development environment” refers to the people, processes and technology associated with system development and integration.

Information Owners and Service Owners must establish secure development environments by considering:

- the sensitivity of data to be processed, stored and transmitted by the system;
- applicable external and internal requirements (e.g. regulations, standards, policies);
- security controls already implemented;
- human resource security;
- the degree of outsourcing;
- the need for segregation between different development environments;
- access control to the environment;
- monitoring of change to the environment and code it stores;
- storing backups at secure offsite locations; and
- control over movement of data to and from the environment.

Outsourced Development

To help ensure that software performs as expected and meet security requirements, Information Owners and Service Owners must implement the following controls when outsourcing development:

- procurement standards and policies for licensing, ownership and intellectual property rights;
- contractual requirements for secure design, coding and testing practices;
- provision of the approved threat model to the external developer;
- acceptance testing for the quality and accuracy of the deliverables;
- provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;
- testing of the software for vulnerabilities and malicious code;
- escrow arrangements if source code is no longer available;
- contractual right to audit development processes and controls; and
- the government remains responsible for compliance with applicable laws and control efficiency verification.

System Security Testing

Information Owners and Service Owners must ensure that new and updated systems require thorough testing and verification during the development processes. A detailed schedule of activities must be prepared with test inputs and expected outputs under a range of conditions.

Tests must initially be performed by the development team. Independent acceptance testing must then be undertaken (for both in-house and outsourced developments) to ensure that the system works as expected and only as expected. The extent of testing must be in proportion to the importance and nature of the system.

System Acceptance Testing

Information Owners and Service Owners must document system acceptance criteria as part of the system development and acquisition process. The criteria include:

- projected performance and resource capacity requirements;
- restart plans and procedures;
- impact on routine operating procedures and manual procedures;
- implementation of security controls;
- assurance that installation of the new system will not adversely affect existing systems particularly at peak processing times;
- training requirements; and
- user acceptance testing.

Protection of Test Data

Test data must be protected and controlled using the same procedures as those in operational systems.

Information Owners must ensure that:

- personal and other sensitive data from operational systems is not used as test data;
- the extraction of test data from operational systems is authorized and logged;
- test data is safeguarded in accordance with its level of sensitivity; and
- data from operational systems is removed from the test environment once testing is complete.

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.