Operations 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 for Operations.

Purpose

To ensure correct and secure operations of information systems, that information systems are protected against malware and loss of data, that events are logged and compliance monitored, that operating system software is controlled, that the exploitation of technical vulnerabilities is prevented, and that the impact of audit activities on operational systems is minimized.

Scope

This policy applies to all Government of Saskatchewan information systems.

Policy Statements

Operational Procedures and Responsibilities

Information Owners and Service Owners must ensure that operating procedures and standards are:

- documented;
- approved by the appropriate authority;
- consistent with government standards and policies;
- reviewed and updated periodically;
- reviewed and updated when there are changes to equipment/systems or changes in business services and the supporting information systems operations; and
- reviewed and updated following a related security incident investigation.

Changes to business processes and information systems that affect information security must be controlled using a change management process compliant with the relevant Standards.

Information Owners and Service Owners are responsible for implementing capacity management processes to monitor and optimize the use of information system resources by:

- documenting capacity requirements and capacity planning processes;
- including capacity requirements in service agreements; and
- monitoring and optimizing information systems to detect impending capacity limit.

Information Owners and Service Owners must project future capacity requirements based on:

- new business and information systems requirements;
- statistical or historical capacity requirements; and
- current and expected trends in information processing capabilities (e.g. introduction of more efficient hardware or software).

Information Owners and Service Owners must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a treat to system security or services.

Development, testing and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational environment.

Protection from Malware

Information Owners and Service Owners must protect GoS Information Systems from Malicious Code by:

- installing, updating and using software designed to scan, detect, isolate and delete malicious code;
- prohibiting the use of unauthorized software;
- checking files, email attachments and file downloads for malicious code before use;
- maintaining business continuity plans to recover from malicious code incidents;
- maintain a critical incident management plan to identify and respond to malicious code incidents;
- maintaining a register of specific malicious code countermeasures (e.g. blocked websites, blocked file extensions, blocked network ports) including a description, rationale, approval authority and the date applied; and
- developing user awareness programs for malicious code countermeasures.

Ministry Security Officers are responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

Backup

Information Owners and Service Owners must define and document backup and recovery processes that consider the confidentiality, integrity and availability requirements of information and information systems. Backup and recovery processes must comply with:

- Ministry business continuity plans (if applicable);
- standards, policy, legislative, regulatory and other obligations; and
- records management requirements.

The documentation for backup and recovery must include:

- types of information to be backed up;
- schedules for the backup of information and information systems;
- backup media management;
- methods for performing, validating and labeling backups; and
- methods for validating the recovery of information and information systems.

Backup media and facilities must be appropriately secured based on a security review or Threat and Risk Assessment.

Logging and Monitoring

Information Owners must ensure that event logs are used to record user and system activities, exceptions and events (security and operational). The degree of detail to be logged must be based on the value and sensitivity of the information and the criticality of the system. The retention time and the resources required to analyze the logs must also be considered.

Event logs may contain sensitive information and therefore must be safeguarded. System administrators must not have the ability to modify, erase or de-activate logs of their own activities.

If event logging is disabled, the decision must be documented. Include the name and position of the approver, date and rationale for de-activating the log. When applicable, update the Privacy Impact Assessment and Threat and Risk Assessment to reflect this decision.

Information Owners must implement controls to protect logging facilities and log files from unauthorized modification, access or destruction. Controls must include:

- physical security safeguards;
- permission for administrators and operators to erase or de-activate logs;
- multifactor authentication for access to sensitive records;
- backup of audit logs to off-site facilities;
- automatic archiving of logs to remain within storage capacity; and
- scheduling the audit logs as part of the records management process.

Event logs must be retained in accordance with the records retention schedule for the information system. Retain them indefinitely if an investigation has commenced or it is known that evidence may be obtained from them

The activities of system administrators, operators and other privileged users must be logged, including:

- the time an event (e.g. success or failure) occurred;
- event details including files accessed, modified or deleted, errors and corrective action taken;
- the account and the identity of the privileged user involved; and
- the system processes involved.

Logs of the activities of privileged users must be checked by the Information Owner or delegate. Checks must be conducted regularly and randomly. The frequency must be determined by the value and sensitivity of the information and criticality of the system. Following verification of the logs, they must be archived in accordance with the applicable records retention schedule.

Clock Synchronization
To ensure that logs are consistent, system administrators must synchronize information system clocks to the local router gateway or a government approved host. System administrators must confirm system clock synchronization following power outages and as part of incident analysis and event log review.

Control of Operational Software
The installation of software on operational information systems must be controlled.

Technical Vulnerability Management
To support technical vulnerability management, Information Owners and Service Owners must maintain an inventory of information assets in accordance with the Asset Management Security Policy. Specific information must be recorded including:

- the software vendor;
- version numbers;
- current state of deployment; and
- the person(s) responsible for the system.

Vulnerabilities which impact government information systems must be addressed in a timely manner to mitigate or minimize the impact on government operations. Service Owners must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- monitoring external sources of information on published vulnerabilities;
- assessing the risk of published vulnerabilities;
- testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- applying corrective measures to address the vulnerabilities; and,
- reporting to the Chief Information Security Officer on progress in responding to vulnerabilities.

Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the change management controls or by following the information security incident response procedures.

Responsibilities for vulnerability response must be included in service agreements with suppliers.

Restrictions on Software Installation
Users are not allowed to install software on government devices unless specifically authorized by a Service Owner or a system administrator.

Service Owners are responsible for the installation of software, updates and patches.

Information Systems Audit Controls
Prior to commencing compliance checking activities such as audits or security reviews of operational systems the Chief Information Security Officer (or designate) and the Information Owner must define, document and approve the activities. Among the items upon which they must agree are:

- the audit requirements and scope of the checks;
- audit personnel must be independent of the activities being audited;
- the checks must be limited to read-only access to software and data, except for isolated copies of system files, which must be erased or given appropriate protection if required when the audit is complete;
- the resources performing the checks must be explicitly identified;
- existing security metrics will be used where possible;
- all access must be monitored and logged and all procedures, requirements and responsibilities must be documented;
- audit tests that could affect system availability must be run outside business hours; and
- appropriate personnel must be notified in advance in order to be able to respond to any incidents resulting from the audit.

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.