Operations 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 Operations.

Table of Contents

1. Operational Procedures and Responsibilities 2

1.1. Documented Operating Procedures 2

1.2. Change Management 2

1.3. Separation of Development, Testing and Operational Environments 3

2. Backup 3

2.1. Information Backup 3

3. Logging and Monitoring 3

3.1. Event Logging 3

4. Control of Operational Software 4

4.1. Installation of Software on Operational Systems 4

Reference Documents

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

- *Operations Security Policy*

1. Operational Procedures and Responsibilities

1.1. Documented Operating Procedures

Operating Procedure documentation must contain detailed instructions regarding:

- information processing and handling;
- system re-start and recovery;
- backup and recovery including on-site and off-site storage;
- exceptions handling, including a log of exceptions;
- output and media handling, including secure disposal or destruction;
- audit and system log management;
- change management including scheduled maintenance and interdependencies;
- computer room management and safety;
- Information Incident Management Process;
- Disaster Recovery;
- Business Continuity Plan; and
- contact information for operations, technical, emergency and business personnel.

1.2. Change Management

Changes must be controlled by:

- identifying and recording significant changes;
- assessing the potential impact, including that on security, of the changes;
- obtaining approval of changes from those responsible for the information system;
- planning and testing changes including the documentation of fallback procedures;
- communicating change details to relevant personnel; and
- evaluating that planned changes were implemented as intended.

Information Owners and Service Owners must plan for changes by:

- assessing the potential impact of the proposed change on security by conducting either a security review or a Threat and Risk Assessment, depending on the size of the change;
- identifying the impact on agreements with business partners and external parties including information sharing agreements, Memoranda of Understanding, licensing and provision of services;
- determining if re-certification or re-accreditation of the information system is required;
- preparing change implementation plans that include test/contingency plans in the event of problems;
- obtaining approvals from affected Information Owners; and
- training technical and operational staff as necessary.

Information Owners and Service Owners must implement changes by:

- notifying affected internal parties, business partners and external parties;
- completing re-certification or re-accreditation prior to implementation;
- training users if necessary;
- documenting the process throughout the testing and implementation phases; and
- confirming the changes have been performed and no unintended changes took place.

1.3. Separation of Development, Testing and Operational Environments

Information Owners and Service Owners must:

- separate operational environments from test and development environments by using different servers, domains and partitions;
- ensure that production servers do not host test or development services or applications;
- prevent the use of test and development identities as credentials for operational systems;
- store source code in a secure location away from the operational environment and restrict access to specified personnel;
- prevent access to compilers, editors and other tools from operational systems;
- use approved change management processes for promoting software from development/test to operational;
- prohibit the use of operational data in development, test or training systems; and
- prohibit the use of sensitive information in development, test or training systems.

2. Backup

2.1. Information Backup

Controls to secure backup media and facilities to be applied after a security review or Threat and Risk Assessment include:

- use approved encryption;
- physical security;
- access controls;
- methods of transit to and from off-site locations;
- appropriate environmental conditions while in storage; and
- off-site locations must be at a sufficient distance to escape damage from an event at the main site.

3. Logging and Monitoring

3.1. Event Logging

Where applicable, event logs must include:

- user ID;
- system activities;
- dates, times and details of key events (e.g. logon, logoff);
- device identity and location;
- logon method;
- records of successful and unsuccessful system access attempts;
- records of successful and unsuccessful data and other resource access attempts;
- changes to system configuration;
- use of elevated privileges;
- use of system utilities and applications;

- network addresses and protocols;
- alarms raised by the access control system;
- activation and de-activation of protection systems (e.g. anti-virus, intrusion detection); and
- records of transactions executed by users in applications.

Event logs may be configured to alert someone if certain events or signatures are detected. Information Owners must establish and document alarm response procedures to ensure they are responded to immediately and consistently. Normally, response to an alarm will include:

- identification of the event;
- isolation of the event and affected assets;
- identification and isolation of the source;
- corrective action;
- forensic analysis;
- action to prevent recurrence; and
- securing of event logs as evidence.

4. Control of Operational Software

4.1. Installation of Software on Operational Systems

To minimize the risk of damage to operational systems Information Owners must implement the following procedures when installing software:

- updates of operational systems must be planned, approved, assessed for impacts, tested and logged;
- a release manager must be appointed to coordinate the install and update of software, applications and program libraries;
- operations personnel and end users must be notified of the changes, potential impacts and, if required, given additional training;
- production systems must not contain development code or compilers;
- user acceptance testing must be extensively and successfully conducted on a separate system prior to production implementation;
- a rollback strategy must be in place and previous versions of application software retained;
- old software versions must be archived with configuration details and system documentation; and
- updates to program libraries must be logged.