Server Security Policy

Last revised: October 2017
Last reviewed: January 2019
Next review: January 2020

Information Security Branch, Ministry of Central Services

This document outlines the Service Security Policy of the Government of Saskatchewan.

Purpose:

The purpose of this policy is to establish the minimum standards for base configurations of server equipment that is owned and/or operated by or for the Government of Saskatchewan (GoS).

Scope:

This policy applies to all server equipment that is owned and/or operated by or for the GoS.

Policy Statements:

The following policy statements apply to the Server Security Policy:

1. General Requirements

All server equipment that is operated by or for the GoS must be owned by an Operational Group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Information Security Branch. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Information Security Branch.

The following items must be met:

- Servers must be registered within the GoS enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location including a backup contact;
  - Hardware and Operating System/Version;
  - Main functions and applications, if applicable.
- Information contained within the GoS enterprise management system must be kept up-to-date.
- Configuration changes for server equipment must follow the appropriate change management procedures.

2. Configuration Requirements

- Operating System configuration should be in accordance with guidelines approved by Information Security Branch.
- Web services or applications should be placed behind a Web Application Firewall.
- Services and applications that will not be used must be disabled where practical.
- Web browsers should be restricted from accessing the internet.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3. **Monitoring**
   - All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
     - All security related logs will be kept online for a minimum of 1 week.
     - Daily incremental tape backups will be retained for at least 1 month.
     - Weekly full tape backups of logs will be retained for at least 1 month.
     - Monthly full backups will be retained for a minimum of 2 years.
   - Security-related events will be reported to Information Security Branch who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
     - Port-scan attacks.
     - Evidence of unauthorized access to privileged accounts.
     - Anomalous occurrences that are not related to specific applications on the host.

4. **Auditing**

   For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic in accordance with the appropriate audit policy.

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, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.