Communications and Network 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 Communications and Networking.

Table of Contents

Reference Documents

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

- *Communications and Network Security Policy*

1. Network Security Management

1.1. Network Controls

1.1.1. Control and Management of Networks

Service Owners must implement network infrastructure security controls and security management systems for networks to ensure the safeguarding of information and information systems. Controls must be selected based on a Threat and Risk Assessment. Assets to be considered include:

- information in transit;
- network infrastructure;
- device configuration, access control definitions, routing information, cryptographic keys;
- network management information;
- network pathways and routes;
- network resources such as bandwidth;
- network security boundaries and perimeters; and
- information system interfaces.

1.1.2. Configuration Control

Service Owners must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords. Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of the following controls:

- encryption;
- access control and multifactor authentication;
- configuration change logs;
- baseline configuration protected by cryptographic checksums;
- configuration ports are to be disabled if not required;
- regular backups; and
- performing status accounting to ensure that configuration baselines reflect actual device configuration.

1.1.3. Trusted Path

Depending on the data classification, information must be transmitted using a trusted path with the following controls:

- data, message or session encryption in accordance with Access Control Security Standards; and
- a means to detect tampering.

1.1.4. Wireless Local Area Networking

Wireless networks must:

- be authorized by Information Technology Division;
- use strong link-layer encryption such as Wi-Fi Protected Access 2;
- ensure that user and device network access are controlled by government authentication services; and
- use strong, frequently changed, automatically expiring encryption keys and passwords.

1.1.5. Equipment Management

Service Owners and suppliers must document responsibilities and procedures for operational management of network infrastructure including devices at network boundaries and in user areas.

1.1.6. Monitoring, Logging and Detection

Centralized log management must be enabled including logging of:

- traffic traversing network security boundaries;
- traffic within networks housing sensitive or mission critical systems or information;
- security events on network devices such as operator login and configuration changes; and
- security events on systems that provide authentication and authorization services to network infrastructure devices (e.g. routers, firewalls, switches).

Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g. automation of log monitoring and alerting).

Devices with the technical capability of remote logging capability (such as syslog or SNMP) are to log access requests to the configuration port.

Service Owners must ensure there is a clear segregation of duties for personnel involved in logging, monitoring and detection activities.

Network discovery tools must be used to monitor and identify unauthorized systems connected to the network.

Active automated surveillance of networks must be implemented to detect and report on security events (e.g. network intrusion).

Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information systems.

1.1.7. Egress Filtering

To prevent interruptions to Ministries’ services caused by unauthorized malicious traffic exiting the partnership network, Service Owners must ensure that:

- egress filtering is enabled;
- egress filtering procedures are reviewed when necessary and adjusted to meet current security best practices; and
- every firewall has a “default deny” rule in use and the principle of least privilege is followed.

2. Information Transfer

2.1. Agreements on Information Transfer

Agreement for information exchange or transfer must define:

- accountability for custody and control;
- authority to publish, grant access to or re-distribute the information;
- purpose and authorized use(s) of the information and software;
- limitations on data linkage;
- duration, renewal and termination provisions;
- primary contacts for agreement, governance and management;
- an agreed labelling system that properly interprets the classification levels of the various parties;
- safeguarding information in accordance with its classification level;
- requirements for handling information (e.g. recording recipients, confirming receipt, reviewing records);
- media management and destruction procedures;
- technical standards for transmission, recording or reading information or software;
- reporting requirements following from security and privacy incidents and breaches;
- liability, accountability and mitigation strategies following from incidents and breaches; and
- problem resolution and escalation processes.