Communications and Network 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 Communications and Networking.

Purpose

To ensure the protection of information in networks and its supporting information processing facilities, and to maintain the security of information transferred within an organization and with any external entity.

Scope

This policy applies to all Government of Saskatchewan communications and networks.

Policy Statements

Network Controls

Service Owners must implement a governance framework that monitors and increases the security posture of the government's networks. A range of controls, compliant with the Communications & Network Security Standards, must be implemented to achieve and maintain security.

Security of Network Services

Formal network service agreements must be established with network service providers. The agreements must specify services offered, service levels, security requirements and security features of network services. They must also specify:

- the schedule for ongoing verification of network security controls;
- the rights of either party to monitor, audit or investigate as needed;
- security incident response, contacts and procedures; and
- the requirement to meet or exceed baseline government security policies and standards.

Service Owners must confirm that specified security features are enabled prior to commencement of service delivery.

Segregation in Networks

Service Owners must segregate services, users and information systems to support business requirements, connectivity and access control. The segregation must be based on the management of risk, and the security principles of the "segregation of duties" and "least privilege".

Service Owners must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

Techniques and technologies selected for network segregation must be based on the findings of a Threat and Risk Assessment. Factors to consider include:

- the sensitivity of the information and system;
- the trustworthiness of the network as revealed by the amount of uncontrolled malicious traffic, the level of device identification and authentication, and the sensitivity to eavesdropping;
- transparency, usability and management costs of network segregation technologies;
- privileged networks (networks with unrestricted or a higher level of access to other networks) must be on a separate network segment physically separated by a firewall; and
- the availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

Information Transfer Standards and Procedures

Users of electronic communication services must comply with the following policies and standards:

- Asset Management, especially where they pertain to acceptable usage;
- Communications & Network Security, especially where they pertain to electronic messaging;
- Security Compliance, especially where they pertain to protection of records.

Users must not forward sensitive government communications outside the government network unless there is a “need-to-know” by the intended recipient.

Users must not forward sensitive government information or communications to externally hosted storage (e.g. cloud storage facilities such as Google Drive) for any reason.

The auto-forwarding of internal email to external addresses is not permitted.

Employees must take appropriate precautions when discussing sensitive information in a telephone call and not leave sensitive information in voice mail or an answering machine.

Information Owners and Service Owners must implement the following controls to further safeguard electronic communications:

- protect information from interception, copying, modification, mis-routing and destruction;
- in accordance with the Operations Security Policy, apply protection against malware that may be transmitted through the use of electronic communication services;
- protect sensitive information that is in the form of an attachment; and
- encrypt information to protect the confidentiality and integrity.

Agreements on Information Transfer

Information Owners and Service Owners must ensure the terms and conditions for exchanging information assets with external parties are documented in an agreement compliant with the relevant Communications and Network Security Standards.

Information or software covered by an exchange agreement must be subjected to a Privacy Impact Assessment and a Threat and Risk Assessment.

Electronic Messaging
The Service Owner must approve implementation of, and modifications to, electronic messaging systems.

To safeguard the integrity of government messages, the electronic messaging services must have a means of:

- protecting messages from unauthorized access, modification or denial of service;
- ensuring correct addressing and transportation of messages;
- providing reliable and available messaging infrastructure; and
- conforming with legislative and regulatory requirements.

Users must:

- use only government electronic messaging services;
- use authorized systems for remote access to government messaging systems;
- use only authorized encryption for email or attachments when required; and
- safeguard sensitive information transmitted via electronic messaging in the same way one safeguards other formats.

Email and other electronic messages may qualify as government records and would thus be subject to The Archives and Public Records Management Act and other legislation, standards and policies. For guidance, refer to the **Provincial Archives of Saskatchewan**.

Government email is automatically archived. For more information, see: *http://www.employeeservices.gov.sk.ca/autoarchiving*.

Confidentiality or Non-Disclosure Agreements
In accordance with Human Resources policies, all employees of executive government must sign the **Oath or Declaration of Office**. The oath includes a statement that the employee will not disclose sensitive government information.

Individuals other than employees must accept and sign an agreement to not disclose sensitive government information. The agreement must contain:

- a description of the information to be protected;
- the expected duration of the agreement;
- the required actions when the agreement is terminated;
- responsibilities and actions of signatories to avoid unauthorized disclosure of sensitive information;
- the permitted use of sensitive information and the rights of the signatory to use it;
- the right of the Government to audit and monitor activities;
- the process for notification and reporting of unauthorized disclosure or other potential breaches;
- terms for information to be returned or destroyed when the agreement is terminated; and
- the expected actions to be taken in case of a breach of the agreement.

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.