Information Transfer 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 Information Transfer.

Purpose

To mitigate the risk that the information may be lost, misappropriated or accidentally released when electronic information is transferred outside of the Government of Saskatchewan (GoS) network.

Scope

This policy states the minimum security requirements for electronic transfer of information across the electronic security perimeter of the GoS network. It applies to Ministries and "prescribed public agencies" supported by the Ministry of Central Services pursuant to **The Information Technology Office Service Regulations**. Where the term "Ministry" is used it means "ministry" as defined by **The Executive Government Administration Act**.

Policy Statements

The GoS recognizes its responsibility to process its information correctly and in line with all legal, regulatory and internal security policy requirements.

Data Classification Required

Electronic information must be classified by the Information Owner before transfer can be considered in order to ensure that the appropriate level of protection can be chosen.

Responsibility Lies with Sender

It is the sender's responsibility to ensure that the risks are properly assessed for what they are intending to do and ensure that all associated risks are adequately understood and covered, that the Information Owner has granted consent, and that the transfer is properly authorized. If a user does not understand the implications of this policy or how it may apply to them, they should seek advice from either their ministry Security Officer or the Information Security Branch.

Agreements on Information Transfer

Agreements must address the secure transfer of business information between the government and external parties.

Information Owners and Service Owners must ensure the terms and conditions for exchanging information assets with external parties are documented in an agreement that defines:

- safeguarding information in accordance with its classification level;
- an agreed labelling system that properly interprets the classification levels of the various parties;
- 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;

- 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;
- problem resolution and escalation processes.

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 thus subject to The Archives and Public Records Management Act and other legislation 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
Requirements for confidentiality or non-disclosure agreements reflecting the government's needs for the protection of information must be identified, documented and regularly reviewed.

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;
- expected duration of the agreement;
- 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
- 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.