# User Responsibilities 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 pertaining to User Responsibilities.*

## Purpose

To communicate the responsibilities that Government of Saskatchewan and its partners have to protect the confidentiality, integrity and availability of government information assets under their control.

## Scope

This policy applies to all authorized users of GoS information technology assets.

## Policy Statements

### Responsibility for Assigned or Accessible Assets

To protect Government computing and information assets:

- passwords must not be shared; users will be held responsible for their actions taken under their assigned user account(s) (i.e. user IDs);
- users will take all reasonable measures to protect any computing and information assets provided by or belonging to the Government of Saskatchewan and will return these items when their use no longer fills a business need, prior to the user's departure or upon request;
- users will observe and honour all applicable intellectual property rights (i.e. copyright, patent, trademark, license agreement) governing the distribution or use of items such as text, graphics, music, or software; and
- users will comply with any published policies for mobile devices and remote access.

### Responsibility for Computing and Network Security

Users will only access accounts, files and data to which they have been provided access or that have been shared for the purpose of public use. The ability to read, execute, modify, delete or copy a file does not imply permission to do so. Accidental access to sensitive information must be reported to the user's management team or organization contact and the information subsequently kept in confidence by the user.

To ensure compliance with software/hardware standards and avoid problems users may not install software, hardware or change system configuration settings without appropriate approval.

### Responsibility to Report Information Security Events

All users of Government systems must report information security events immediately to the Information Technology Division Service Desk. Examples of events include, but are not limited to:

- breach of information confidentiality, integrity or availability expectations;
- non-compliance with policies or guidelines;
- breaches of physical security;
- access violations;
- malicious software; and
- lost or stolen information assets.

Information security events reported to a Ministry by a supplier must be further reported to Information Security Branch.

**Acceptable Use and Limited Personal Use**

Government of Saskatchewan information systems exist to conduct the business of Government. This is their core use.

Users must comply with applicable federal and provincial legislation and policies and standards of the Government of Saskatchewan.

Authorized use includes:

- activities necessary to perform one's official duties;
- career development and other professional activities.

Incidental use is permitted when it is on personal time, does not incur any costs to Government, does not interfere with the business of Government and does not compromise the integrity of government information and/or systems.

Unacceptable use includes, but is not limited to:

- attempting to circumvent the configuration of security software or hardware;
- installing hardware or software unless specifically authorized;
- conducting activities that could bring the public service into disrepute or harm the Government's reputation;
- using Government systems for personal gain (inclusive of but not limited to gambling, operating a business, and executing investment transactions);
- conducting activities that contravene the law;
- conducting activities that negatively impact the operation of Government systems;
- disclosing personal, personal health or other sensitive information about others, without authorization;
- displaying, accessing or distributing pornographic, other offensive content or anything that would not survive public scrutiny or disclosure;
- conducting activities that expose the Government to civil liability;
- communicating a personal belief, the subject matter of which may be provocative, politically sensitive, offensive, derogatory towards others, or perceived as representing the views of the employer (except when it is part of your job responsibilities to do so);
- conducting activities that contribute to personal harm of others such as harassment or bullying.

**Notifications**

Authorized users of Government of Saskatchewan systems must be aware of the following:

- Systems are monitored to manage network traffic, ensure systems are operating as intended, detect faults, detect internal and external threats, and to ensure compliance with policies and standards.
- There is an expectation of privacy regarding the content of emails and personal files. Routine network monitoring does not involve access to this information.
- Special monitoring may be permitted without notice to the user where illegal or other unacceptable use is suspected. This special case monitoring must be authorized by the appropriate Ministry officials.

## 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.