Human Resources 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 Human Resources.

Purpose

Prior to employment, to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. During employment, to ensure that employees and contractors are aware of and fulfil their information security responsibilities. At termination or change in employment, to protect the government's interests as part of the process of changing or terminating employment.

Scope

This policy applies to all personnel with access to Government of Saskatchewan information and assets.

Policy Statements

Personnel screening must be performed prior to entering a working relationship with the Government of Saskatchewan.

All new employees and contractors must be screened. The screening must be conducted in accordance with relevant legislation and Human Resource Policies of the Government of Saskatchewan. The screening must include verification of:

- identity;
- education, skills and experience;
- employment history; and
- character references.

A criminal record check must be conducted in accordance with **Section PS 816** of the Human Resource Manual.

All personnel must be made aware of and agree to the Government of Saskatchewan's expectations related to information security.

The terms and conditions for employees of the Government of Saskatchewan are described in the **Ethics and Conduct** section of the Employee Services Portal. The Oath of Office includes an entry regarding the protection of sensitive information and must be signed by the employee.

The terms and conditions for contractors and external party users must include:

- a confidentiality or non-disclosure agreement;
- legal responsibilities and rights;
- responsibilities for the classification of information and management of government assets;
- responsibilities for the handling of external party information; and
- responsibilities for the handling of personal information and personal health information.

Managers must ensure that the terms and conditions of employment are agreed to by all personnel.

Management must ensure that personnel apply security in accordance with standards, policies and procedures.

Managers must support the Government's information security objectives by:

- briefing all personnel on their security roles and responsibilities prior to granting access to sensitive data and systems;
- ensuring all personnel have access to these Information Security Standards; and
- ensuring all personnel conform to the terms and conditions of employment.

Employees must be made aware of the protections provided by the **Public Interest Disclosure Act (2011)** regarding the reporting of wrongdoings.

Personnel must be given appropriate information security training and be informed of changes to standards, policies and procedures.

Managers must include an information security awareness component during orientation for new personnel.

Ongoing awareness training must be conducted. Among the topics that must be discussed are:

- safeguarding sensitive government information;
- known threats to information security;
- legal responsibilities;
- information security standards, policies, directives and guidelines;
- how to report information security events;
- appropriate use of government information and assets;
- related disciplinary processes; and
- how to obtain security advice.

There must be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

When it is determined that an employee or contractor was responsible for a security breach or a violation of standards or policies, Information Security Branch must notify the appropriate Ministry Security Officer.

Appropriate personnel in the Ministry must review details of the incident, consider disciplinary action if warranted and arrange for permanent or temporary removal of access privileges when appropriate.

The **Human Resources Manual Section 803** defines Corrective Discipline processes in the Government of Saskatchewan.

Managers must advise personnel of their information security responsibilities when employment changes or is terminated.

Terminated employees and contractors must be made aware of:

- ongoing security requirements including the need to not disclose sensitive government information;
- legal responsibilities;
- responsibilities described in confidentiality or non-disclosure agreements; and
- any other applicable policy, standards, or contract.

Managers can find applicable instructions and forms on the **Employee Services Centre** site.

When users accept different job responsibilities within government the current Manager must ensure that Ministry information assets are turned over to the Ministry. Ensure that access to systems and services in the current Ministry is revoked.

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. Policy exceptions will be reviewed on a periodic basis for appropriateness.