Foundational Security Principles

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the foundational security principles of the Government of Saskatchewan.

Policy Statements

The Government of Saskatchewan will manage its information and related data assets in a disciplined and organized manner to optimize government business operations. As a result, appropriate security behaviors will effectively support and enable service delivery to customers.

The Government of Saskatchewan will ensure Information Security by:

- Implementing a risk management approach to investment prioritization;
- Becoming a trusted advisor to customers;
- Optimizing the portfolio of IT investments, which allows the ITD to ensure that an enterprise approach to IT security is integrated;
- Continuously improving IT service delivery, which allows the ITD to create an environment for citizen-centric service delivery that is secure and based on the changing nature of threats within the environment.

Foundational Security Principles

Principles provide an anchor for building security programs and are intended to guide security decisions.
A successful implementation of information security embodies the following principles:

- Central coordination of IT security allows for the proper development of enterprise solutions and monitoring;
- Information Security will be practiced through a unified enterprise approach across government, which will create efficiencies and decrease costs through the creation of economies of scale and scope;
- Using modern, fit-for-use security and information protection technologies for the enterprise;
- Information Security processes and procedures will be readily adaptable to react to technology changes and unexpected events;
- Security is everyone's responsibility;
- Security must reflect asset value and risk;
- Security requires a multi-layered defense strategy;
- System and data access privileges must match job function;
- Security is only as strong as the weakest link;
- Security follows the principles of "least privilege" and "separation of duties" with regard to performing security functions;
- Access to and transmission of data or resources should be secured, audited and monitored at a level consistent with its sensitivity as reflected by its data classification;
- Any individual or service accessing sensitive data or resources, as defined by security policy and data classification, as well as legislative, regulatory and contractual requirements, should be positively identified;
- The recipient of sensitive data is responsible for maintaining the security of the data;

- The implementation of security controls is founded upon a solid understanding of information security requirements, threat and risk assessment, and risk management;
- Security will reduce the implementation time for projects by utilizing a common set of authentication, authorization, encryption technologies and, methodologies for new projects (application and infrastructure); and
- Information security policy, objectives, and activities reflect and enable business objectives.