Access Control 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 Access Control.

Purpose

To ensure proper and effective use of logical and physical access controls to safeguard access to GoS networks, application, and information.

Scope

This policy applies to all GoS use of access controls including users and service providers.

Policy Statements

To limit access to government information and information systems, access to information systems and services must be consistent with business needs and based on security requirements:

- The Government of Saskatchewan must control access to information, information systems and business processes. Access must be authorized, managed, monitored and controlled on the basis of business needs and security requirements. Security controls to safeguard the confidentiality, integrity and availability of information and information assets must be implemented appropriate to the data classification level.
- Access to Government information and information systems must be appropriate for the user's job description and role. It must consider the "need-to-know" and "least privilege" principles. In all cases there must be a method to validate the identification of the user.
- Users must only be provided with access to the networks and networks services that they have been specifically authorized to use.

To ensure authorized users access appropriate resources and to prevent unauthorized access to systems and services, there must be a formal user registration and de-registration process for granting access to all information systems:

- Enhanced user security screening or background checks must be completed prior to granting access when justified by the value and sensitivity of the asset or the findings of a Threat and Risk Assessment.
- There must be a formal user access provisioning process for assigning or revoking access rights to all information systems.
- The allocation and use of privileged access rights must be restricted and controlled for privileged users.
- The issuance of authentication credentials must be controlled through a formal management process.
- Information Owners must formally review user access rights at regular intervals.
- The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.
- When a user terminates or transfers within the organization employee directories and other documentation must be updated to reflect this change.
- Stale account reports must be distributed by Service Owners to the appropriate Information Owners on a prescribed schedule.

To make users accountable for safeguarding their authentication information:

- Users must follow the government's standards in the selection and use of passwords.

To prevent unauthorized access to systems and applications:

- Access to information and information systems functions must be restricted in accordance with the access control security standards and specifications.
- Every information system must have an access control policy that specifies access permissions for information and system functions. Information Owners and Service Owners are responsible for developing and implementing the access control policy for their business applications. The access control policy must specify:
  - the information controlled;
  - the system functions controlled; and
  - the roles authorized to access the resource and what types of access are permitted (e.g. Read, Write, Execute, Delete).
- System utilities or functions that can bypass user access controls must be specified in the access control policy. Access to them must be restricted.
- Information that is publicly accessible must be segregated from sensitive information.
- Access to information systems and applications must use a secure logon process.
- A password management system must be implemented to provide an effective, interactive means of ensuring quality passwords.
- Use of system utility programs must be restricted and tightly controlled.
- Access control must be maintained for program source libraries.

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.