Access Control Security Standard

Information Security Branch, Ministry of Central Services

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

This document outlines the Government of Saskatchewan security standards for Access Control.

Table of Contents

Reference Documents

The following documents are available on the IT Security Services Taskroom:

- *Access Control Security Policy*
- *Access Control Security Specification*

Government of Saskatchewan

1. Business Requirements of Access Control

1.1. Access Control Standard

Information Owners and Service Owners must:

- develop, document and implement procedures for the issuance of user IDs and user access rights to information and information systems;
- ensure that access to information and information systems is based on business needs and appropriate for the job responsibilities and role of the user(s);
- segregate the duties of administering access control, e.g., separate access request, access authorization and access administration and assign a business owner/approver for each;
- remove or revoke access rights when required in accordance with Section 2.2;
- review user access rights in accordance with Section 2.5;
- document the business requirements to exceed the existing access control rules and rights for each user or group of users;
- complete an inventory of business applications and all related information and information systems in accordance with Section 1.1; and
- ensure user access rights to each system are documented in accordance with Section 4.1.

Users must:

- ensure that computing devices are accessed only by those authorized to do so;
- ensure that computing devices are password-protected in accordance with Section 3.1;
- shut down all applications and logoff the network at the end of a shift or when not returning to the work area for an extended period;
- lock unattended computers with a password-protected screensaver or other approved mechanism in accordance with the policies and standards for Physical and Environmental Security; and
- comply with the Information Technology Acceptable Usage Policy (refer to ***Section PS 1103*** of the Human Resource Manual) in accordance with the policies and standards for Asset Management.

1.2. Access to Networks and Network Services

Information Owners and Service Owners must ensure that:

- users are granted access to only those networks required to fulfill their job responsibilities;
- access to networks is authorized in accordance with Section 1.1;
- users authenticate to networks in accordance with Section 4.2;
- procedures are implemented to protect access to networks and network services;
- access to networks, including remote access, is in accordance with standards published by Information Technology Division; and
- network services are monitored for compliance with this Section and unauthorized access attempts.

2. User Access Management

2.1. User Registration and De-registration

2.1.1. Registration

Information Owners must manage access to information assets under their control. They must implement a user registration process which:

- ensures access requests are approved by the supervisor/manager of the user requesting access;
- ensures the reasons for requesting access are consistent with the duties of the user;
- ensures access is approved via the service request fulfillment processes;
- maintains records of access approvals;
- ensures personnel understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- ensures access rights are consistent with the data uses documented in a Privacy Impact Assessment where applicable;
- ensures access is traceable to an identifiable individual or process;
- ensures each user is assigned a single unique user ID for accessing information systems;
- ensures that responsibilities for authorizing access are segregated from granting access;
- restricts access based on pre-defined role permissions; and
- provides secure and separate transmission of the user ID and password.

2.1.2. De-registration

Information Owners must formally assign responsibilities and implement processes to:

- remove access privileges for employees no longer with the organization;
- promptly review access rights whenever a user changes duties and responsibilities;
- promptly review access rights whenever the user's branch or Ministry is involved in significant reorganization;
- review access privileges for employees on extended absence or temporary assignments within ten working days of the change of status;
- remove access privileges for employees terminated for cause concurrent with notification to the individual; and
- periodically check for and remove inactive or redundant user accounts.

2.2. User Access Provisioning

The provisioning process for assigning or revoking access rights granted to user IDs must include:

- obtaining authorization from the Information or Service Owner for the use of that system;
- verifying that the level of access granted is in accordance with Section 1;
- verifying that the level of access granted is consistent with the policies and standards for Organization of Information Security covering the segregation of duties and related requirements;
- ensuring that access rights are not activated before authorization procedures are completed;
- maintaining a central record of access rights granted a user ID;

- adapting access rights of users who have changed roles and immediately removing or blocking access rights of users who have left government (Section 2.6); and
- periodically reviewing access rights with Information Owners (Section 2.5).

2.3. Management of Privileged Access Rights

2.3.1. Granting System Privileges

Information Owners and Service Owners must authorize the granting of system privileges. They must:

- identify and document the system privileges associated with each information system or service;
- ensure the process for requesting and approving access to system privileges includes management approval(s) prior to granting of system privileges;
- ensure processes are implemented to remove system privileges from users concurrent with changes in job status (e.g., transfer, promotion, termination);
- limit access to the fewest number of users needed to operate or maintain the system or service;
- ensure the access rights granted are limited to and consistent with the users' job function and responsibilities;
- maintain a record of users granted system privileges;
- ensure use of system privileges is recorded in audit logs that cannot be altered by the privileged user;
- implement processes for ongoing compliance checks of the use of system privileges; and
- regularly review authorizations in place to confirm that access is still needed and that the least number of users needed have access.

Local admin privileges are distinct from privileged access rights and must follow the appropriate process to be granted.

2.3.2. Access Control Standard for Local Admin on Desktops

Requests for local admin privileges must have business justification. Each request must be authorized by the Security Officer for the Ministry.

2.4. User Password Management

Service Owners must formally designate individuals who have the authority to issue and reset passwords. They must adhere to the following controls:

- passwords may only be issued to users whose identity has been confirmed prior to issuance;
- individuals with the authority to issue or reset passwords must transmit new passwords to the users in a secure manner (e.g., using approved encryption);
- temporary passwords must be changed on first use;
- users must not be asked to disclose their passwords;
- passwords must never be stored in an unprotected manner (i.e. use approved encryption and/or appropriate physical security); and
- default passwords provided by technology vendors must be changed to one that is compliant with government standards.

2.5. Review of User Access Rights

Information Owners must implement processes to regularly review access rights to information and information systems. Access rights must be reviewed:

- at least annually;
- more frequently for privileged users and for systems with the highest sensitivity;
- when a user's status changes due to promotion, demotion, re-assignment, transfer, removal from a user group or other change that impacts that user's need to access information;
- as part of a major re-organization;
- with the introduction of new technology or applications; and
- when the access control procedures are changed.

Review of access rights must include:

- confirmation that access is based on the "need-to-know" and "least privilege" principles;
- review and verification of access control lists; and
- confirmation that changes to access rights are logged and can be audited.

2.6. Removal or Adjustment of Access Rights

Information Owners and Service Owners must review access to information systems and information processing facilities when personnel change employment, including:

- when personnel assume new roles and responsibilities,
- during restructuring of positional or organizational roles and responsibilities,
- when personnel begin long-term leave.

Information Owners and Service Owners must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment by:

- removing or modifying physical and logical access,
- recovering or revoking access devices, cards and keys.

Information Owners and Service Owners must ensure access to information systems and information processing facilities is reduced or removed before the employment terminates or changes based upon the evaluation of risk factors such as:

- whether the termination or change is initiated by the user or by management,
- the reason for termination,
- the current responsibilities of the user, and
- the value of the assets currently accessible.

3. User Responsibilities

3.1. Password Use

Users must:

- change temporary passwords at first logon;
- select complex passwords in accordance with the standards described below;
- use a unique password (one that is for government business only and not the same as one that is for personal use);
- change passwords at specified intervals;
- not disclose passwords to anyone else;
- not write down passwords unless they are safeguarded with appropriate and approved physical security;
- not keep an electronic file of passwords unless it is safeguarded with approved encryption; and
- change their passwords immediately after a suspected or actual compromise.

3.2. Password Standards

Account passwords must, at a minimum:

- have at least eight characters;
- contain characters from at least three of the following categories:
    - English uppercase letters (A – Z);
    - English lowercase letters (a – z);
    - numbers (0 – 9);
    - non-alphanumeric symbols (e.g.: !,#,$,%); and
    - Unicode characters;
- not contain three or more characters from the user's account name.

The password must be changed at least every ninety days. When supported by the operating system password history must be enabled and at least the previous seven passwords must be remembered and not reused. The minimum password age can be any value.

User accounts must be locked after five invalid login attempts. A locked account can be unlocked using the password reset tool or by contacting the Service Desk.

4. System and Application Access Control

4.1. Information Access Restriction

Information system access controls must be configurable so that access permissions can be modified without making code changes.

4.2. Secure Logon Procedures

Logon processes must be configured to:

- not display details about backend systems prior to successful completion of the logon process;
- display a banner prior to logon warning that the computer must only be accessed by authorized users and that activities are monitored;
- comply with the Password Standards in Section 3.1;
- not display passwords in clear text as they are entered;
- validate logon information only on completion of all input data;
- record unsuccessful logon attempts;
- limit the number of unsuccessful logon attempts before locking the account;
- activate a password lock after a maximum of fifteen minutes of inactivity, requiring the user to re-authenticate, where applicable;
- prevent brute force logon attempts;
- not transmit passwords in clear text over a network; and
- information classification will determine the technical requirements for logon configuration processes.

4.3. Password Management System

Password management systems must:

- enforce the use of individual user IDs and passwords;
- support user selection and change of passwords in compliance with the Government of Saskatchewan Password Standards (Section 3.1);
- enforce the change of the temporary password at first logon or a password reset by an administrator;
- enforce password changes at the specified interval including advance notice of expiry;
- maintain a record of previous passwords and prevent re-use;
- not display the password on the screen when being entered;
- store password files separately from application system data;
- include protection from unauthorized access and manipulation; and
- store and transmit passwords in protected (e.g. encrypted) form.

4.4. Use of Privileged Utility Programs

Information Owners and Service Owners must limit the use of system utility programs by:

- defining and documenting authorization levels;
- restricting access to the minimum number of trusted, authorized users;
- periodically reviewing the status of users with permissions to use them;

- ensuring their use maintains segregation of duties;
- requiring a secure logon process;
- ensuring they are identified and their access logged;
- segregating them from application software where possible; and
- removing or disabling unnecessary and obsolete system utilities and software.

4.5. Access Control to Program Source code

Program source code is code written by programmers which is compiled and linked to create executables. Associated items are designs, specifications, verification and validation plans.

Access to program source code and associated items must be controlled by:

- ensuring that, where possible, program source libraries are not held in production environments;
- establishing procedures for the management of program source code and libraries;
- ensuring that support personnel do not have unrestricted access to program source libraries;
- safeguarding system documentation;
- authorizing the updating of program source libraries and associated items;
- authorizing the issuance of program source code to application developers;
- logging the modification of program source code; and
- ensuring that the maintenance and copying of program source libraries is subject to strict change control procedures in accordance with the policies and standards for System Acquisition, Development and Maintenance.