Access Control Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Information Security Branch

Last revised: April 2021
Last reviewed: April 2021
Next review: April 2022

Purpose

The purpose of this policy is to ensure users have the appropriate access levels specifically authorized to them to access information on systems and applications and that individuals understand the responsibility their access level provides them. This policy defines access control standards for system use notices, remote access, and definition and documentation of relationships for information systems.

Scope

This Access Control Policy applies to all business processes and data, information systems and components, personnel, and physical areas of the Government of Saskatchewan. Person(s) this policy applies to include but are not limited to:

- All employees, whether employed on a full-time or part-time basis by the Government of Saskatchewan
- Contractors and Service Providers

Definitions

This section intentionally left blank.

Governing Laws, Regulations, and Standards

Guidance	Section
ISO/IEC 27001:2013	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)
NIST SP 800-53 v4	AC-1~AC-25
NIST SP 800-171	3.1.1-3.1.22

Policy Statements

Basic Security Requirements:

- The Government of Saskatchewan will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- The Government of Saskatchewan will limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

- The Government of Saskatchewan will control the flow of non-public information (NPI) following the approved authorizations.
- Formal user registration and de-registration process must be developed and initiated to allow the assignment of rights.
- The duties of individuals will be separated to reduce the risk of malevolent activity without collusion.
- The Government of Saskatchewan will employ a role-based access method.
- The principle of least privilege will be employed, including for specific security functions and privileged accounts.
- Non-privileged accounts or roles will be used when accessing non-security functions.
- The Government of Saskatchewan will prevent non-privileged users from executing privileged functions and audit the execution of such functions.

To Prevent Unauthorized Access to Systems and Applications:

- Access to information and information systems functions must be restricted following 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 login process.
- A password management system must be implemented to provide an effective, interactive means of ensuring quality passwords.
- The use of system utility programs must be restricted and tightly controlled.
- Access control must be maintained for program source libraries.
- Privileged access rights will be allocated in a highly controlled and restricted process. Their usage will also be controlled.
- Upon termination of employment, an employee's or external party's user access rights will be revoked.
    - The Government of Saskatchewan will employ automated processes to remove temporary and emergency accounts after a determined amount of time. A similar automated process will exist for disabling inactive accounts.
- Asset owners must conduct regular reviews of users' access rights and use of accounts.
- Unsuccessful login attempts will be limited.
- Stale account reports must be distributed by Service Owners to the appropriate Information Owners on a prescribed schedule.
- The time and date of logins and account changes will be appropriately recorded and monitored.
- To prevent access/viewing of data after a period of inactivity, the Security Awareness Training Procedure will use a session lock with pattern-hiding displays.
- A user session will remain locked for a predetermined time or until the user re-establishes access through an established authentication procedure.
- A user session will terminate (automatically) after a defined condition.
- The Government of Saskatchewan will provide privacy and security notices consistent with applicable NPI rules.
- Password management systems will be interactive and mandate strong passwords.
- Any use of utility programs capable of overriding system and application controls will be highly controlled and restricted, if necessary.
- Any access to program source code will be strictly prohibited.

- Remote access sessions will be monitored and controlled.
- Cryptographic mechanisms to protect the confidentiality of remote access sessions will be employed.
- The Government of Saskatchewan will route remote access via managed access control points.
- The Government of Saskatchewan will authorize remote execution of privileged commands and remote access to security-relevant information.
- The Government of Saskatchewan will authorize wireless access before allowing such connections.
- Wireless access will be protected using authentication and encryption.
- The Government of Saskatchewan will control the connection of mobile devices.
- The Government of Saskatchewan will encrypt NPI on mobile devices.
- Connections to and use of external information systems will be verified, controlled, and limited.
- There will be limited use of organizational portable storage devices on external information systems.
- The Government of Saskatchewan will control the information posted or processed on publicly accessible information systems.
- The Government of Saskatchewan will implement appropriate data mining prevention controls.

Relevant Procedures

This section intentionally left blank.

Non-Compliance

In cases where it is determined that a breach or violation of Government of Saskatchewan 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 a review and acceptance of risk by the Security Governance Committee. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Branch. Policy exceptions will be reviewed periodically for appropriateness.

Revision History

Version ID	Date of Change	Author	Rationale