SNOWBE ONLINE #010
PRIVILEGED ACCESS POLICY

Sean Redding

Privileged Access Policy -

Version # 1.0

10-12-25

Table of Contents

Purpose

The purpose of this policy is to establish protocols for managing Privileged Access to IT Resources, ensuring adherence to the Principle of Least Privilege, and promoting transparency, accountability, and security across SnowBe Online through thorough documentation, review, and auditing of access requests.

Scope

SnowBe Online requires all faculty, staff, and administrators to follow the principle of least privilege, which ensures that each user has only the minimum necessary permissions to perform their job responsibilities. Supervisors must regularly review their staff's access to data and services and ensure that permissions are set at the lowest required level.

Definitions

Local Administrator Account: A non-domain account with full access to directories, files, services, and other resources on a local computer.

Principle of least privilege: A user, program, or process should have only the minimum necessary permissions to perform a function.

Role-Based Access Controls (RBAC): Limits data or network access based on an employee's or user's specific roles or responsibilities.

Separation of duties: The requirement for more than one person to complete a specific task to prevent theft or misuse of resources.

Roles & Responsibilities

IT Director / IT Manager:

Are responsible for the continued development, implementation, dissemination, and maintenance of information security policies, procedures, security controls, and control techniques to address the Access Control process. Responsible for ensuring that the approved administrative and technical privacy controls are in place and effective. Responsible for educating employees about their access control responsibilities.

IT Team:

The IT Team is responsible for the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability of data.

Employees:

Employees are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use, or modification of IT Resources (theft, fraud, or misuse of facilities).

Vendors/Third Parties:

Vendor and third-party service providers must ensure that all IT systems and applications developed for the State comply with this policy and any other applicable Enterprise Information Technology Policies, Standards, and Procedures.

Policy

The principle of least privilege shall be employed, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with the organization's missions and business functions. Least privilege applies to the development, implementation, and production lifecycle of information systems. The following shall be done:

a) Only authorized individuals shall perform updates to restricted or confidential data, such as citizen and business databases. Authorized personnel include security administrators, system and network administrators, system maintenance personnel, system programmers, and other privileged users.

b) SnowBe Information Systems shall prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

1. Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.

2. Non-privileged users are individuals who do not possess appropriate authorizations.

3. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

c) Administrators of multi-user systems, systems that allow for concurrent usage of the system by multiple persons, must have at least two user credentials. One of these user credentials must provide privileged access, with all activities logged; the other must be a normal user credential for performing the day-to-day work of an ordinary user.

AC- 6 (1) – Least Privilege | Authorize Access to Security Functions

Access to security functions and security-relevant information shall be explicitly authorized. Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

AC- 6 (2) – Least Privilege | Non-Privileged Access for Nonsecurity Functions

Users of SnowBe's information system accounts, or roles, with access to sensitive information, shall use non-privileged accounts or roles when accessing non-security or non-privileged functions. This control enhancement limits exposure when operating from within privileged accounts or roles.

AC-6 (5) – Least Privilege | Privileged Accounts

Privileged accounts on SnowBe's information system shall be restricted to a limited number of authorized individuals with a need to perform administrative duties. Privileged accounts, including superuser accounts, are typically described as system administrators for various types of systems.

a) Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions using role-based access control (RBAC).

AC-6 (7) – Least Privilege | Review of User Privileges

The following requirements shall be implemented to review user privileges:

a) Review of standard user accounts at least annually and privileged user accounts at least semi-annually; and

b) Reassign or remove privileges, if necessary, to correctly reflect agency mission and business needs.

AC-6 (9) – Least Privilege | Log Use of Privileged Functions

Misuse of privileged functions, either intentionally or unintentionally, by authorized users or by unauthorized entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Information systems shall log the execution of privileged functions.

AC-6 (10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Information systems shall prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

Exceptions/Exemptions

Requests for an exception must be submitted in writing to consult with the IT Director or IT Manager.

The request must be detailed with information, including:

- Length of time
- Policy or standard
- Reason

Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.

If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.

The IT Director and the Commissioner must maintain constant communication during the exception. If approved, the Commissioner's office will send the letter of approval to the requester with details. In the event of denial, a letter of explanation will be sent to the requester with the reason the IT Director denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-12-25	IT Director	IT Director	Initial draft of policy.

Citations

https://semo.edu/finance-admin/_pdfs/finadm-10-15-policy.pdf

NIST Special Publication 800-53 Revision 5

https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment