SNOWBE ONLINE
Policy# AC-01
Policy and Procedures

Daphnie Bruno

Policy #AC-01 - Version # 1.1

November 05, 2024

Table of Contents

Purpose

The purpose of this guide is to provide guidance for the Policy and Procedures controls identified in NIST SP 800-53. The guide provides SnowBe Online employees, contractors with significant security responsibilities and other IT personnel involved in implementing access control, guidance on the specific procedures they are to follow for implementing AC features and functions for systems under their purview.

Scope

The requirements outlined within this guide apply to and must be followed by all SnowBe Online employees, contractors, vendors, and third party services who are involved in implementing access control features and functions for SnowBe Online systems and information. All Snowbe Online systems must adhere to the requirements and guidance provided with regard to the procedures, processes, and methods for implementing access control as described in this guide.

Definitions

Dissemination

This is higher diction compared to simpler alternatives like "distribution" or "sharing." It is often used in formal documentation.

Facilitate

Slightly elevated compared to simpler alternatives like "support" or "enable," though it fits in a professional context.

Guidance

This word is slightly more formal than "instructions" or "advice," but it's common in professional documents.

NIST 800-53 Rev. 5

A comprehensive set of security and privacy controls provided by the National Institute of Standards and Technology (NIST). This framework is designed to protect federal information systems and organizations, as well as non-governmental entities that follow federal guidelines. It addresses access control, least privilege, and other key security measures.

Oversee

More formal than "supervise" or "monitor," though common in business settings.

Purview

This word can sometimes be considered higher diction because it's less common in everyday speech, but it's standard in professional contexts.

Roles & Responsibilities

Chief Information Security Officer (CISO)

- Manage the development, documentation, and dissemination of the Department-level IT system access control policy.
- Review and update the policy annually and following significant changes in threats, laws, or technologies.
- Ensure alignment with federal laws, executive orders, and regulations.

Compliance Officer

- Ensure the access control policy and procedures comply with relevant laws and regulations.
- Assist in reviewing and updating the policy to maintain compliance.

Employees

- Adhere to the access control policy and procedures.
- Participate in required training related to access control.
- Report any suspected violations or security incidents.

Human Resources

- Coordinate with IT and Security teams for employee onboarding and offboarding processes.
- Ensure timely communication of employee status changes that affect access rights.

IT Security Manager

- Oversee the implementation of access control policies and procedures.
- Ensure regular audits and reviews of access control measures.
- Coordinate with other departments to maintain effective access control.

IT Security Officer

- Develop and maintain system-specific access control procedures.
- Conduct regular reviews of access rights and privileges.
- Investigate and respond to access control-related security incidents.

IT Staff:

- Implement and maintain technical access control measures.
- Assist in user account management and access rights assignment.
- Provide technical support for access control-related issues.

Management:

- Support and enforce the access control policy across the organization.
- Approve access requests for their respective departments.
- Ensure their staff complies with access control policies and procedures.

Third-Party Vendors:

- Comply with the organization's access control policies when accessing systems.
- Provide documentation of their own access control measures when relevant.
- Report any security incidents or violations related to access control.

Policy

This policy has been created to establish and maintain a comprehensive framework for managing access control across SnowBe Online's. This policy defines the guidelines and procedures for managing access to all SnowBe Online systems, applications, data, and physical resources.

Policy Statements:

AC-1.1 SnowBe Online shall develop, document, and disseminate to all employees, contractors, and authorized users:

a) An organization-wide access control policy.
b) Procedures to facilitate the implementation of the access control policy and associated controls.

AC-1.2 All SnowBe Online systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions.

AC-1.3 Access control mechanisms must be based on the principle of least privilege, ensuring users have only the minimum access necessary to perform their job functions.

AC-1.4 Supervisors of SnowBe Online employees and contractors are responsible for:

a) Coordinating and arranging system access requests for all new or transferring employees.
b) Verifying an individual's need-to-know (authorization).
c) Modifying or terminating access for transferring or terminating personnel.

AC-1.5 Data or system owners must grant access to systems based on:
a) A valid need-to-know/need-to-share determined during the account authorization process.
b) The intended system usage.
c) Alignment with job responsibilities and organizational policies.

AC-1.6 The access control policy and procedures shall be reviewed and updated:
a) At least annually
b) Following the identification of evolving threats
c) Upon issuance of new or significantly changed existing federal laws, executive orders, directives, regulations, or SnowBe Online policies.

AC-1.7 SnowBe Online shall establish and maintain an inventory of all information system accounts, including their authorized users and the access rights granted.

AC-1.8 Regular audits of user access rights shall be conducted to ensure compliance with the principle of least privilege and to identify and remove unnecessary access permissions.

AC-1.9 All access to SnowBe Online systems must be logged and monitored, with anomalies or suspicious activities investigated promptly.

AC-1.10 This policy applies to all SnowBe Online information systems, including those operated or maintained on behalf of SnowBe Online by third parties.

Responsibilities:

a) The Chief Information Security Officer (CISO) is responsible for developing, implementing, and maintaining this policy.
b) IT Security is responsible for implementing and enforcing technical controls to support this policy.
c) Human Resources is responsible for notifying IT of personnel changes that may affect access rights.
d) All employees, contractors, and authorized users are responsible for complying with this policy.

AC-1: Policy and Procedures Enhancement

- N/A

Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will be in place until the policy changes or the person's employment status changes.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Enforcement

Violations of this IT Security Plan will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	05-Nov-24	Daphnie Bruno		Created and updated document sections
1.1	09-Nov-24	Daphnie Bruno		Updated Policies and finalized documents

Citations

- https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- https://www.gsa.gov/system/files/Access-Control-(AC)-%5BCIO-IT-Security-01-07-Rev-5%5D-08-18-2022.pdf
- https://www.ed.gov/sites/ed/files/fund/contract/about/acs/2023-ac-access-control-standard.pdf
- https://www.ed.gov/sites/ed/files/fund/contract/about/acs/2023-ac-access-control-standard.pdf