SNOWBE ONLINE Policy# AC-3 Access Enforcement Control

Humberto Gonzalez

Version # 2.0

DATE: July 14, 2024

Table of Contents

Purpose

The purpose of this policy is to ensure that access to SnowBe Online's information systems and data is strictly enforced by existing security standards. This policy is intended to prevent unwanted access, safeguard sensitive information, and guarantee that all access is properly regulated and monitored.

Scope

This policy applies to all employees, contractors, and third-party vendors who have access to SnowBe Online's information systems and data.

Definitions

Control Enhancement: Augmentation of a security or privacy control to build in additional but related functionality to the control, increase the strength of the control or add assurance to the control.

Information Security: The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Least Privilege: The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Mandatory Access Control: An access control policy that is uniformly enforced across all subjects and objects within a system. A subject that has been granted access to information is constrained from passing the information to unauthorized subjects or objects; granting its privileges to other subjects; changing one or more security attributes on subjects, objects, the system, or system components; choosing the security attributes to be associated with newly created or modified objects; or changing the rules for governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints. Mandatory access control is considered a type of non-discretionary access control.

Role-Based Access Control: Access control based on user roles (i.e., a collection of access authorizations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or several individuals.

Roles & Responsibilities

- Employees: Must comply with access enforcement regulations and report any suspicious activity or violations.

- IT Department: Responsible for overseeing the technical aspects of the security program, including the implementation and maintenance of security controls, system hardening, patch management, network security, and data protection through encryption and backups.

- Senior Management/Executive Team: Sets the tone and direction for information security, and assigns resources to secure information assets.

- Third-Party Vendors: Must comply with SnowBe Online's access enforcement standards and ensure that their access is limited to only the resources required for their job. Access concerns or breaches must be notified immediately.

Policy

Access to SnowBe Online's systems and data must be restricted and enforced to maintain security and compliance with organizational regulations. Access enforcement measures must be created to guarantee that users only have access to resources that are required for their responsibilities.

- **Mandatory Access Control -** To avoid unauthorized data disclosure, this policy limits interactions between subjects (people or processes) and objects (devices, files, and records) by implementing obligatory access control. Access to both classified and unclassified information is strictly controlled, and the least privilege principle is upheld. Access permissions will be assigned based on user roles, with automatic restrictions in place for unauthorized access attempts. Regular audits will be conducted to ensure compliance with MAC policies.

- **Role-Based Access Control:** By ensuring users only access the information required for their work, this policy improves security by streamlining privilege administration and allocating access permissions based on job descriptions. It encourages the disciplined management of user credentials and the avoidance of unwanted access. Employees must submit formal access requests that are reviewed and approved by their managers and the IT security team. Access permissions will be reviewed bi-annually to ensure they align with current job roles and responsibilities. All employees will receive training on access policies and the importance of adhering to role-based access principles.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
2.0	07/14/2024	Humberto Gonzalez	Robin Groff Alarcon	Access Enforcement Control Policy Implemented.

Citations

Brief Description for control enhancement reference- AC: Access Control - CSF Tools

Enforcement- Sample Detailed Security Policy (bowiestate.edu)

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

NIST SP 800.53 R5- Security and Privacy Controls for Information Systems and Organizations (fso-lms4-immortal-assets.s3.us-east-1.amazonaws.com)

Purpose/Introduction- Michigan Technological University Information Security Plan (mtu.edu)

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)