SNOWBE ONLINE Policy# AC-6
Least Privilege Control

Humberto Gonzalez

Version # 2.0

DATE: July 14, 2024

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 3

POLICY 3

EXCEPTIONS/EXEMPTIONS 4

ENFORCEMENT 4

VERSION HISTORY TABLE 4

CITATIONS 5

Purpose

This policy is intended to guarantee that SnowBe Online workers, contractors, and third-party entities have access to only the information and resources required for their specialized tasks. This policy attempts to minimize the possibility of unauthorized access or data breaches by implementing the principle of least privilege.

Scope

This policy governs all employees, contractors, and third-party entities 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.

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.

Network Access: Access to a system by a user (or a process acting on behalf of a user) communicating through a network, including a local area network, a wide area network, and the Internet.

Privileged Access: Access that allows an individual who take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, or other such employees whose job duties require access to sensitive data residing on a system or network. This data can be paper or electronic data. For this policy, application and other developers are also considered privileged.

Privileged Command: A human-initiated command executed on a system that involves the control, monitoring, or administration of the system, including security functions and associated security-relevant information.

Security Functions: The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Roles & Responsibilities

- Employees: Make sure the least privilege policy is followed, and report any unauthorized access.

- 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: Adhere to the least privilege policy by limiting their access to what is required for the contracted services. Vendors must also notify SnowBe Online immediately if they encounter any access difficulties or breaches.

Policy

At SnowBe Online, the least privilege principle needs to be applied to every system and application. Making sure users only have access to the information and platforms required for their jobs and responsibilities.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with all relevant laws, policies, and regulations. In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.

Non-privileged accounts and roles are to be used for daily functions such as but not limited to email or internet browsing. This requirement limits exposure when operating from within privileged accounts or roles.

- **Authorized Access To Security Functions -** This policy makes sure that only authorized individuals, like security administrators, system administrators, and privileged users, have access to security features like audit settings, intrusion detection parameters, and system account management. Access permissions for these functions will be granted and reviewed by designated personnel.

- **Network Access to Privileged Commands** - To safeguard privileged commands, all network access (as opposed to local access) to these commands will be controlled and secured. Authorized users accessing privileged commands remotely must use secure connections and authentication methods.

- **Non-Privileged Access For Non-security Functions -** To reduce exposure and ensure effective access control measures, such as role-based access control, non-privileged accounts must be used for non-security-related functions, including general system use, communication, and browsing.

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	Least Privilege Access 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)

Least Privilege- Privileged Access Policy (uc.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)