SNOWBE ONLINE POLICY AC-6
LEAST PRIVILEGE

Ydali Hernandez

AC-6 – Version 1.0

July 11, 2024

Table of Contents

Purpose

The purpose of this policy is to ensure the security of SnowBe Online's data and systems by implementing the principle of least privilege and separation of duties. This policy outlines the responsibilities of employees and administrators in maintaining secure access to data and services.

Scope

This policy applies to all services and data within SnowBe Online. It mandates the implementation of a Role-Based/Privilege-Based framework to ensure that user permissions are set at the lowest necessary level for job functions. The policy requires the management of company-provided devices, including determining software installation, data access, and user login permissions. Each department is responsible for limiting staff access to data and services based on job responsibilities. Elevated permissions are granted only when needed and must be removed once the task is complete or no longer required. A centralized log collection application or SIEM must be used to maintain and monitor all relevant logs for systems and applications, tracking inappropriate access to data or devices. New applications or services, whether in-house, commercial, or cloud-based, must provide access to data. Exceptions to this policy will be addressed by the Assistant Vice President of Information Technology on a case-by-case basis.

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 and responsibilities.
Security Information Events Management (SIEM): An information security tool that stores and maintains important log files and provides real-time analysis of security alerts generated by applications and network hardware.
Separation of Duties: The requirement for more than one person to complete a specific task to prevent theft or misuse of resources.

Roles & Responsibilities

Assistant Vice President of Information Technology:
Address exceptions to this policy on a case-by-case basis.
Ensure compliance with the policy across all departments.
Department Heads:
Limit staff access to data and services based on job responsibilities.
Regularly review staff access to data and services to ensure permissions are set at the lowest required level.
Employees:
Adhere to the principle of least privilege and use only the permissions necessary for their job

functions.
Report any security incidents or policy violations to the IT department immediately.

IT Department:

Implement and maintain the Role-Based/Privilege-Based framework.
Manage company-provided devices, including software installation, data access, and user login permissions.
Ensure all logs are collected and monitored through a centralized SIEM application.
Update and maintain the company's technical infrastructure, including firmware, patches, antivirus, and backup software.
Secure servers in a locked area and update the WordPress Shopping cart.

Policy

SnowBe Online implements a Role-Based/Privilege-Based framework where all employees have access permissions set at the lowest necessary level for their job functions, with elevated permissions granted and promptly removed as needed. The IT department manages company-provided devices, overseeing software installation, data access, and user login permissions. Department heads must regularly review and adjust staff access to ensure minimal required permissions. A centralized SIEM application monitors all relevant logs, with logs older than three months archived to cloud storage. The IT department maintains and updates all network devices, PCs, and servers, ensuring anitivirus and backup software are current and securing servers in locked areas. PCI compliance is enforced, and new applications must provide role-based access to data. Mobile devices are reviewed and approved for data access. The Assistant Vice President of Information Technology addresses policy exceptions on a case-by-case basis.

Exceptions/Exemptions

To request an exception or exemption, the individual must submit their request to the department manager, who then will forward it to the IT department manager. The request must include a detailed explanation of the necessity for the exception or exemption, covering the business or technical reasons that justify the deviation from the standard policy.
The IT Manager will review the request to ensure all required information is provided and will assess the potential security impact. A formal risk assessment will be conducted to evaluate the implications of the requested exception or exemption.
The IT Manager will then either approve or deny the request. The duration for the exception or exemption will be 18 months unless the requester specifies otherwise. Additionally, the exception or exemption will be subject to periodic reviews to ensure it remains necessary and that security risks are adequately managed.

Enforcement

Violations of this policy will result in disciplinary actions.

1st offense: Write up
2nd offense: Write up and training courses
3rd offense: Write up and leave without Pay

4th offense: Termination

Devices that do not comply with the security policy will be disconnected from the network until compliance is achieved.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	07/11/24	Ydali Hernandez	R. Alarcon	Initial draft of the policy document.

Citations

AVP Information Technology (2011, October 28). *UB Network Connection Policy*. University at Buffalo. Retrieved July 5, 2024, from https://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/ub-network-connection.html

Michigan Tech (2011, October 13). *Information Security Plan*. Michigan Technological University. Retrieved July 5, 2024, from https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

NIST (n.d.). *Security and Privacy Controls for Information Systems and Organizations*. DOI. Retrieved July 11, 2024, from https://fso-lms4-immortal-assets.s3.us-east-1.amazonaws.com/1411/20216/4d126967-102f-4196-9748-1ac71939bed4-98b487b5-5406-4175-857f-95beef5e4ea6/NIST.SP.800-53r5.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIARE7PEONU35M5ITYW%2F20240711%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240711T195450Z&X-Amz-Expires=3600&X-Amz-Signature=e965f820325a9b14bb4e9c778403ba5c86a2fad1efa0cfc6aee8e656eb57ca77&X-Amz-SignedHeaders=host&response-content-disposition=inline%3B%20filename%3D%22NIST.SP.800-53r5.pdf%22&x-id=GetObject

SEMO (n.d.). *Least Privilege Policy*. Southeast Missouri State University. Retrieved July 11, 2024, from https://semo.edu/finance-admin/_pdfs/10-15-policy-least-privilege-policy-v8-ready.pdf

University of Colorado (n.d.). *IT Security Program*. Retrieved July 5, 2024, from https://www.cu.edu/ope/aps/6005