SNOWBE ONLINE Policy 11.10
Access Enforcement

Alex Fhermaye

Access Enforcement – 11.10

Version: 1.1

DATE: June 17, 2024

11.10 Access Enforcement – V 1.1
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Alex Fhermaye
DATE: June 17, 2024

Table of Contents

Purpose

The purpose of the Access Enforcement Security Policy at SnowBe is to establish a comprehensive framework for controlling and managing access to the company's information systems, networks, and data. This policy aims to safeguard sensitive information, ensure compliance with relevant regulatory requirements, and protect the integrity, confidentiality, and availability of SnowBe's digital assets. By defining clear roles, responsibilities, and procedures for access control, the policy seeks to mitigate risks associated with unauthorized access, data breaches, and other security threats, thereby supporting the overall mission and operational effectiveness of SnowBe.

Scope

This policy is comprehensive in scope and applies to the entire SnowBe Online community. This includes, but is not limited to, Directors, Department Heads, Team Leads, employees, temporary employees, contractors, volunteers, and guests who have access to any of SnowBe Online's information technology resources. These resources encompass a wide range of assets critical to our operations and security.

Information technology resources include, but are not limited to, all forms of data, images, text, and software. These may be stored on various types of hardware such as servers, workstations, laptops, mobile devices, and other electronic devices. Additionally, this policy covers information stored on non-digital mediums such as paper documents and other physical storage media.

The protection of these assets is paramount to ensuring the confidentiality, integrity, and availability of information, which are the cornerstones of our security posture. This policy sets forth the guidelines and procedures for safeguarding these assets against unauthorized access, disclosure, alteration, and destruction. It is designed to be comprehensive, covering all possible scenarios and providing a clear framework for maintaining and enhancing our information security measures.

Every member of the SnowBe Online community is responsible for understanding and adhering to these guidelines. This responsibility includes recognizing the importance of these resources and the role each individual play in protecting them. By following this policy, we collectively contribute to maintaining the trust of our clients, partners, and stakeholders, and to ensuring the smooth and secure operation of our business processes.

This policy is not static; it is reviewed and updated regularly to adapt to new security challenges and technological advancements. All changes will be communicated promptly to ensure that every member of our community is aware of their responsibilities and the importance of compliance. By adhering to this policy, we uphold SnowBe Online’s commitment to excellence in information security.

Definitions

Access Controls:

Security techniques and measures that regulate who or what can view or use resources in a computing environment.

Availability:

The assurance that information and resources are accessible to authorized users when needed.

Compliance:

The act of adhering to and demonstrating adherence to laws, regulations, guidelines, and specifications relevant to its business processes.

Enhancement:

Refers to an additional feature or improvement that builds upon the base control to provide more specific, stringent, or comprehensive security measures.

Information Assets:

Data, images, text, or software stored on hardware, paper, or other storage media that hold value to SnowBe Online.

Integrity:

The assurance that information is accurate, complete, and has not been altered in an unauthorized manner.

Exception Request Form:

A formal document used to request deviations from established IT security policies.

Legal, Regulatory, and Industry Standards:

Set of laws, regulations, guidelines, and specifications established by regulatory authorities or industry groups to ensure security, privacy, and operational efficiency.

NIST 800-53:

A publication that provides a catalog of security and privacy controls for federal information systems and organizations.

Patch:

A piece of software designed to update or fix problems with a computer program or its supporting data, including fixing security vulnerabilities and other bugs.

Risk Assessments:

The process of identifying, evaluating, and estimating the levels of risk involved in a situation, followed by coordinated efforts to mitigate and manage the risk.

Security Controls:

Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Roles & Responsibilities

Chief Information Officer (CIO)

- Develop and implement the overall IT security strategy in alignment with business objectives.
- Oversee the IT department to ensure effective execution of security policies and controls.
- Ensure compliance with industry standards and regulatory requirements, including NIST 800-53 and PCI DSS.

Compliance Officer

- Ensure the company adheres to all relevant legal, regulatory, and industry standards.
- Conduct regular audits and assessments to identify compliance gaps.
- Work with other departments to implement corrective actions and maintain compliance.

IT Consultant

- Provide expert advice and guidance on IT security best practices and frameworks.
- Conduct risk assessments and develop action plans to address identified vulnerabilities.
- Assist in the implementation of security controls, policies, and procedures.

IT Security Manager

- Oversee the day-to-day operations of IT security within the company.
- Manage the IT security team and ensure the implementation of security controls and measures.
- Monitor security incidents and respond to breaches or threats.

Sales Team

- Adhere to IT security policies and procedures, particularly when accessing company systems remotely.
- Report any suspicious activities or potential security incidents to the IT security team.
- Ensure the secure handling of customer data and payment information during transactions.

System Administrator

- Manage and maintain servers, ensuring they are secure and up-to-date.
- Implement and enforce access controls to limit data access based on roles and responsibilities.
- Regularly update and patch operating systems and software to mitigate vulnerabilities.

Web Developer

- Ensure the company’s website and applications are secure and up-to-date.
- Implement security measures for online transactions and data storage.
- Regularly update and patch the WordPress shopping cart and other web components.

Policy

AC-3 Access Enforcement

SnowBe is dedicated to strong access controls to keep its information systems secure and confidential. This policy sets the rules and expectations for managing access to SnowBe's digital resources. Access to SnowBe's systems, applications, and data will be granted based on the principle of least privilege, meaning people only get the minimum access needed for their job. We will use various methods to monitor and control access to SnowBe's resources, including authentication, authorization, and auditing processes. These methods help prevent unauthorized access and detect any attempts to breach the system. SnowBe will use both discretionary and mandatory access controls to manage permissions and protect sensitive information.

This document exists to create a clear framework for access enforcement at SnowBe. It is crucial for protecting the company's information systems, networks, and data from unauthorized access and security breaches. By setting clear rules and procedures, this policy ensures that all access to sensitive information and resources is controlled, monitored, and restricted based on the principles of least privilege and need-to-know. It outlines how we will use role-based access control, restrict access to specific information types, and combine discretionary and mandatory access controls. This helps protect SnowBe's digital assets, comply with regulations, and strengthen the company's overall security.

Enhancement 7 – Role-based Access Control

SnowBe will implement Role-based Access Control (RBAC) to manage user permissions based on their job roles. Each role will be assigned specific access rights tailored to the responsibilities and requirements of the position. This ensures that employees only have access to the information and systems necessary for their role, reducing the risk of unauthorized access.

Enhancement 11 – Restrict Access to Specific Information Types

Access to specific types of sensitive information will be restricted based on the user's role and the need to know. This policy ensures that only authorized personnel can access critical data, such as financial records, customer information, and proprietary business information. Additional safeguards, such as encryption and multi-factor authentication, will be applied to protect these data types.

Enhancement 15 – Discretionary and Mandatory Access Control

SnowBe will employ a combination of discretionary access control (DAC) and mandatory access control (MAC) to regulate access to its systems and data. DAC allows resource owners to decide who can access their resources, providing flexibility in managing permissions. MAC enforces access policies based on predefined security classifications, ensuring that users can only access information for which they have proper clearance. This dual approach enhances security by combining user discretion with stringent policy enforcement.

Exceptions/Exemptions

At SnowBe Online, we recognize that there may be exceptional circumstances requiring deviations from our established IT security policies. However, such exceptions/exemptions are not guaranteed approval and must be carefully evaluated to ensure they do not compromise our security posture. The following outlines the process for requesting and managing exceptions/exemptions:

How to Request an Exception/Exemption

1. All requests for exceptions or exemptions must be submitted in writing via the official IT Security Exception Request Form, available on the company net.

2. A detailed explanation of why the exception or exemption is being requested, including the specific policy or control from which the deviation is sought. The proposed duration for which the exception or exemption is needed.

Approval Process

1. The IT Security Manager will review the request to ensure it includes all required information and assess the potential risks and impacts.

2. The Chief Information Officer (CIO) has the final authority to approve or deny exceptions and exemptions. In cases involving significant risk, the CIO may consult with the Chief Executive Officer (CEO) or the IT Security Advisory Committee.

3. The applicant will be notified in writing of the decision, including any conditions or additional controls required as part of the approval.

Duration and Review

1. Approved exceptions or exemptions will typically be granted for a specified duration, not exceeding one year unless otherwise stated.

2. All active exceptions or exemptions will be reviewed periodically by the IT Security Manager to ensure that they remain necessary and that any associated risks are being adequately managed.

Enforcement

Compliance with the IT security policy and any granted exceptions or exemptions will be monitored continuously. Any deviations from approved exceptions or exemptions must be reported immediately to the IT Security Manager. Failure to follow the IT security policy, including the proper procedure for requesting and adhering to exceptions or exemptions, may result in disciplinary actions. Penalties may include, but are not limited to, revocation of access privileges, formal reprimand, or other disciplinary actions up to and including termination of employment.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	June 4, 2024	Alex Fhermaye	Joe Ramos	Initial Submission for review
1.1	June 17, 2024	Alex Fhermaye	Joe Ramos	Template converted to Access Enforcement Policy

Citations

AC-3. STIG Viewer | Unified Compliance Framework®. (n.d.). https://www.stigviewer.com/controls/800-53/AC-3

Force, J. T. (2020, December 10). *Security and Privacy Controls for Information Systems and organizations*. CSRC. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final