SNOWBE ONLINE SECURITY PLAN

Group Member Names:

Jacob Barrera Section 01
Chris Denney Section 01
Justin Himes Section 01
León Masters Section 02
Davon Kincey Section 01
Pedro Hernandez Section 01

Table of Contents

Section 1: Introduction

The purpose of this plan is to guarantee the confidentiality, integrity, and availability of data while supporting SnowBe Online's goals and legal obligations. Information security policies serve as strategies to handle and implement security, stop fraud, and ensure business stability. This plan reflects SnowBe Online's obligation to protect sensitive information.

Section 2: Scope

This plan applies to the entire SnowBe Online community, including all employees, contractors, volunteers, and guests who have access to SnowBe Online information technology resources. It encompasses both online and in-person interactions. The scope includes the SnowBe Online network and all related systems and devices that interact with it.

The assets covered by this plan include data, images, text, and software, stored on various media such as hardware, paper, or other storage devices. These assets are crucial to the operations and security of SnowBe Online and must be protected to ensure business continuity and integrity.

Section 3: Definitions

Access Control: The process of controlling access to systems, networks, and information based on business and security requirements.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Control Activities: The policies, procedures, techniques, and mechanisms that help ensure management's response to reduce risks identified during the risk assessment process is carried out.

Encryption: The process of converting information so that it is humanly unreadable except by someone who knows how to decrypt it.

Information Assets: Definable pieces of information in any form, recorded or stored on any media that is recognized as valuable to the organization.

Integrity: Guarding against improper information modification or destruction, ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Risk Assessment: A process to determine what information technology resources require protection and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Section 4: Roles & Responsibilities

Chief Information Security Officer (CISO)

- Lead the company's security efforts and make sure they meet business and legal requirements.
- Approve security policies and handle major security issues.
- Report on security risks and incidents to the leadership team.

Department Managers

- Approve employee access based on job needs.
- Let the IT Department know if someone's role changes or they leave the company.
- Make sure their teams follow the security rules.

Employees

- Follow security rules and training.
- Use strong passwords and keep accounts private.
- Report anything suspicious or unusual to IT.
- Keep company devices secure and use them responsibly.

IT Department

- Set up and manage security tools like firewalls, antivirus, and encryption.
- Control and monitor access to company systems and data.
- Fix security issues and keep systems updated.
- Watch for threats and respond quickly to security problems.

Security Team

- Check for risks and find ways to improve security.
- Keep an eye on the network for unusual activity.
- Plan and test how the company will respond to security incidents.
- Train employees to stay safe online.

Technical Consultant

- Employs controls using the NIST 800-53 framework and presents security advancement suggestions.

Third-Party Vendors

- Follow SnowBe Online's security rules and agreements.
- Use company systems only for approved tasks.
- Report any security issues immediately.

Section 5: Statement of Policies, Standards and Procedures

Policies

AC-1 - Policy and Procedures: Establishes the access control policy and procedures for SnowBe Online.

AC-2 - Account Management: Manages and controls user accounts, including their creation, modification, and deletion.

AC-3 - Access Enforcement: Enforces access control policies to ensure authorized access to systems and data.

AC-6 - Least Privilege: Ensures users have the minimum access necessary to perform their duties.

AC-7 - Unsuccessful Logon Attempts: Implements measures to handle unsuccessful logon attempts to protect against unauthorized access.

AC-8 - System Use Notification: Provides notifications regarding the acceptable use of the system to users upon login.

AC-9 - Previous Logon Notification: Notifies users of the previous logon to help identify potential unauthorized access.

AC-10 - Concurrent Session Control: Limits the number of concurrent sessions for users.

AC-11 - Device Lock: Ensures devices lock after a specified period of inactivity to prevent unauthorized access.

AC-12 - Session Termination: Terminates user sessions after a defined period of inactivity.

AC-16 - Security and Privacy Attributes: Manages and enforces security and privacy attributes associated with system resources.

AC-17 - Remote Access: Provides guidelines for secure remote access to SnowBe Online's systems.

AC-18 - Wireless Access: Establishes security measures for wireless access to the network.

AC-19 - Access Control for Mobile Devices: Ensures the secure use of mobile devices to access the network.

AC-20 - Use of External Systems: Provides policies for the use of external systems and resources.

AC-21 - Information Sharing: Defines the process and policies for sharing information securely.

AC-23 - Data Mining Protection: Protects against unauthorized data mining activities.

AC-24 - Access Control Decisions: Specifies how access control decisions are made and enforced.

AC-25 - Reference Monitor: Ensures that access control decisions are enforced consistently and effectively.

AU-9 - Protection of Audit Information: Ensures the protection of audit information from unauthorized access, modification, and deletion.

CM-3 - Configuration Change Control: Ensures that changes to system configurations are properly managed and authorized.

CP-9 - System Backup: Provides guidelines for regular backups of system data and information. Essential for ensuring data availability and recovery in case of data loss or corruption.

IA-3 - Device Identification and Authentication: Ensures that devices accessing the network are properly identified and authenticated. Crucial for preventing unauthorized access and maintaining network security.

IA-7 - Cryptographic Module Authentication: Ensures that cryptographic modules used for authentication are validated and secure.

MA-4 - Nonlocal Maintenance: Provides guidelines for secure remote maintenance of systems. Essential for ensuring the security and integrity of systems during remote maintenance activities.

PCI Policy: This PCI Compliance Policy is designed to provide guidance on the importance of protecting payment card data and customer information at SnowBe Online. The policy exists to ensure that SnowBe Online complies with the Payment Card Industry Data Security Standard (PCI DSS), thereby minimizing risks associated with the processing, storage, and transmission of cardholder data.

SA-9 - External System Services: Provides guidelines for the secure use of external system services. Important for ensuring third-party services meet security requirements.

SC-8 - Transmission Confidentiality and Integrity: Ensures that data transmitted over networks is protected against interception and tampering. Crucial for protecting sensitive information during transmission.

SC-12 - Cryptographic Key Establishment and Management: Ensures the secure generation, distribution, and management of cryptographic keys.

SC-13 - Cryptographic Protection: Provides encryption to protect sensitive information both at rest and in transit.

SC-16 - Transmission of Security Attributes: Ensures the transmission of security attributes alongside data to maintain its security properties.

SC-28 - Protection of Information at Rest: Focuses on protecting sensitive information stored on devices or media.

SI-4 - System Monitoring: Provides guidelines for continuous monitoring of systems to detect and respond to security incidents.

SI-7 - Software, Firmware, and Information Integrity: Ensures the integrity of software, firmware, and information.

SI-19 - Deviation Detection and Monitoring: Ensures the detection and monitoring of deviations from expected system behavior.

SP-1: Acceptable Use Policy: Defines acceptable use of IT resources to ensure security and compliance with SnowBe Online standards.

SP-2: Access Control: Establishes procedures for granting, managing, and terminating access to company systems and data.

SP-3: Backup Policy: Ensures that SnowBe Online can safely and securely back up mission-critical data and recover it in the event of a disruption.

SP-4: Bring Your Own Device Policy: Defines the responsibilities and acceptable use of

personal devices accessing SnowBe Online's resources.

SP-5: Clean Desk Policy: Ensures that sensitive information is not left unattended and is properly secured when not in use.

SP-6: Confidentiality Policy: Outlines measures for protecting sensitive company information from unauthorized disclosure.

SP-7: Data Breach Response Policy: Defines the procedures to respond to a data breach to minimize impact and recover operations.

SP-8: Data Classification Policy: Provides a systematic approach to classify and protect data based on its sensitivity and criticality.

SP-9: Data Retention Policy: Specifies the duration for which company data should be retained and the procedures for its disposal.

SP-10: Disaster Recovery: Details the processes and procedures to recover and protect IT infrastructure in the event of a disaster.

SP-11: Email Policy: Establishes guidelines for the appropriate use of company email systems to ensure security and professionalism.

SP-12: Employee Awareness and Training Policy: Promotes awareness and training for employees on security practices and procedures.

SP-13: Firewall Policy: Outlines the requirements for firewall configuration and management to protect SnowBe Online's network.

SP-14: Incident Response Policy: Defines the actions to be taken in response to security incidents to minimize impact and recover operations.

SP-15: Network Security Policy: Establishes security measures to protect the integrity, confidentiality, and availability of SnowBe Online's network.

SP-16: Password Management Policy: Sets the standards for creating, managing, and protecting passwords to secure access to systems.

SP-17: Personnel Security Policy: Outlines measures to ensure the security and integrity of personnel handling sensitive information.

SP-18: Remote Access Policy: Provides guidelines for securely accessing SnowBe Online's systems remotely.

SP-19: Risk Management Policy: Identifies and mitigates risks to SnowBe Online's operations, assets, and data.

SP-20: Secure Systems Management Policy: Details procedures for managing and securing IT systems to protect against threats.

SP-21: Third-Party Vendor Management Policy: Outlines the process for assessing and managing risks associated with third-party vendors.

SP-22: Vulnerability Management Policy: Establishes procedures for identifying, assessing, and addressing vulnerabilities in SnowBe Online's IT systems.

SP-23: Password Protection Policy: Specifies the requirements for protecting passwords to ensure secure access to company systems.

SP-24: Acceptable Encryption Policy: Defines acceptable encryption standards to protect sensitive data during storage and transmission.

Standards and Procedures

P-1 Create a Password Procedure: The purpose of this Password Procedure is to outline detailed steps for developing and managing strong, secure passwords to protect user accounts and sensitive information from unauthorized users.

P-2: New Account Creation Procedure: Standardize, secure and efficient create user account process. All employees, contractors, and third-party service provider shall adhere to this, respecting any internal policies, legal requirements and standards set forth to support access controls and sensitive information.

S-1 Create a Password Standard: The objective of this Password Standard is to secure the establishment and usage of strong, secure passwords that will protect user accounts and any kind of sensitive information from being accessed by unauthorized persons

Section 6: Exceptions/Exemptions

Exceptions and exemptions to SnowBe Online's security policies are granted on a case-by-case basis and are not guaranteed. Each request will be carefully evaluated to ensure it aligns with the company's overall risk management strategy and compliance requirements. Approved exceptions or exemptions must not create unacceptable security risks or regulatory violations and will be subject to regular review.

1. **How to Request an Exception or Exemption**
    - Submit a written request detailing the policy or control in question, the reason for the request, proposed mitigations, and the requested duration via the designated request platform (e.g., Service Desk or email to IT Security Team).
    -
2. **Why an Exception or Exemption is Requested**
    - Provide a clear justification, including specific business, technical, or operational reasons that make adherence to the policy impractical or detrimental.
3. **Who Can Approve an Exception or Exemption**
    - Exceptions or exemptions must be approved by the IT Director or IT Manager. In some cases, approval may also require input from the Risk Management or Compliance team.
4. **How Long the Exception or Exemption Will Be in Place**
    - Specify the duration of the exception or exemption, including an expiration date. Temporary exceptions will be reassessed before renewal or termination. Permanent exemptions must undergo periodic review to ensure continued relevance and safety.

Section 7: Version History Table

Version	Date	Description
1	11/27/2024	First edit
1.1	12/1/2024	Added policies
1.2	12/2/2024	Added details
1.3	12/9/2024	Added PCI Access Control Policies
1.3.1	12/22/2024	Added create a password procedure and standard

Citations

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf

https://www.cl.cam.ac.uk/archive/rja14/Papers/security-policies.pdf

https://www.bowiestate.edu/files/resources/information-security-public.pdf