SNOWBE ONLINE SECURITY PLAN

Group Member Names:
Miya Ferguson [Group Leader]
Devin Jimenez
Sean Redding
~~Alisa Jacobs~~

Version #4 10-23-25

Table of Contents

Introduction

This Information Security Plan discusses the safeguards in place for the company SnowBe to protect the confidentiality, integrity, and availability of information and devices. This document is designed to keep SnowBe in line with federal guidelines, data protection acts, institutions, and state. These safeguards aim to:

- Strengthen security controls
- Improve network security
- Apply relevant security frameworks
- Limit user access to critical systems
- Patch and manage vulnerabilities
- Define acceptable use in the workplace
- Prepare for, detect, and respond to security incidents
- Manage vulnerabilities through policies
- Implement ongoing security awareness and training

Scope

This security plan applies to all employees, contractors, systems, businesses, and locations of SnowBe. As well as third-party agents, service providers, and affiliates that store, transmit, and have access to SnowBe information. As well as any hardware devices like servers, endpoint devices, software, and network devices that handle SnowBe data.

Definitions

Access Enforcement (AC-3) – The process of guaranteeing that users, processes, or devices (subjects) can only interact with information, resources, or systems (objects) for which they have approved authorization.

Attribute-Based Access Control (ABAC) – An access enforcement model that grants or denies access based on a combination of attributes belonging to the subject, object, requested action, and environmental conditions.

Cryptographic Mechanisms (AC-17(2)) – Security measures implemented to protect the confidentiality and integrity of data transmitted during remote access sessions (I.e., encryption).

Endpoint Device – any device used to initiate a remote connection to the SnowBe network, which includes the thirty sales laptops and approved mobile devices.

IRP – Incident Response Plan.

IT – Information Technology VPN – Virtual Private Network.

Least Privilege (AC-6) – The security principle of granting users or system processes only the minimum level of access necessary to perform their authorized functions.

Managed Access Control Point (AC-17(3)) – An authorized and centrally managed network device (I.e., VPN

or Firewall) through which all remote access connections must be routed.

NIST 800-53 - A catalog of security privacy controls for U.S federal information systems developed by the National Institute of Standards Technology

Object – A passive entity within the system that contains or receives information, such as a file, record, database, or system component (e.g., The Credit Card Database).

PCI DSS – Payment Card Industry Data Security Standard

Physical Access Audit Log – A record maintained at physical entry and exit points to track who accessed the facility or secured area and when.

Remote Access (AC-17) – Any connection to a SnowBe information system or network resource that originates outside the secure, managed boundary of the main office.

Role-Based Access Control (RBAC) – An access enforcement model where access decisions are granted or denied based on the formal roles assigned to the subject (e.g., Accountant and Customer Support).

Subject – An active entity within the system, such as a user, a program, or a process acting on behalf of a user, attempting to gain access.

Virtual Private Network (VPN) – A cryptographic mechanism used to establish a secure, encrypted connection over a public network (i.e., The Internet).

Roles & Responsibilities

Employees – Maintain compliance, report incidents, and complete regular security and awareness training.

Executives – Responsible for maintaining policies and approving them.

IT Personnel/Security Team – Maintain physical and technical controls, conduct risk monitoring, and enforce policies.

Statement of Policies, Standards, and Procedures

Policies

Physical Security - #001

- Physical Security policy is implemented in the main office in LA, specifically targeting the security of the internal server infrastructure. It will be implemented by locking the six servers in a secured area of the office and enforcing access authorization to that area in addition to the main facility controls.

Security Training and Awareness - #002

- This policy is used to counteract SnowBe's documented "laid-back culture" and personnel being a major vulnerability due to neglected controls. It will be implemented by mandating annual security literacy training for all personnel and specialized role-based training for employees handling sensitive PII and the new access controls.

Media Protection - #003

- Ensure the security of all SnowBe digital and physical media containing company or customer data throughout its entire lifecycle. This control is crucial for SnowBe to prevent unauthorized access or disclosure of sensitive information like the indefinitely stored customer data and purchase history, by mandating proper storage and sanitization procedures for all devices and storage media.

Remote Access - #004 (AC-17)

- This policy is necessary because SnowBe's business model relies on highly mobile workforce, with thirty laptops utilizing a VPN to log into the office to access company applications. This policy also establishes strong encryption, routed through managed access points and actively monitored for suspicious activity.

Network Segmentation/Access Control - #005 (AC-3)

- Counteracting consultant's finding that "most employees had universal access" by enforcing the use of Role-Based Access Control (RBAC) across the network. This is essential for logically separating sensitive data (e.g., stored credit cards) from general employee access, minimizing the blast radius of any breach, and ensuring compliance with all required PCI compliance item.

Patch and Vulnerability Management - #006

- To actively protect SnowBe's systems by ensuring that all network devices, PCs, and Windows servers are kept up to date with the latest patches and firmware. This is vital for mitigating risk posed by the consultant's finding of neglected patches and firmware, thereby decreasing the attack surface and defending against known security threats.

PCI DSS - #007

- The company accepts and stores all credit cards on its website database, making it immediately subjected to the Payment Card Industry Data Security Standard. This policy will mandate technical and

procedural controls to secure cardholder data (i.e., strong encryption and restricted access) to prevent financial fraud and meet the required PCI compliance items suggested by the technical consultant.

Access Enforcement - #008 (AC#17)

- Access enforcement is needed to protect sensitive information and assets by limiting access to only authorized individuals. Without it, SnowBe Online could face significant security risks, legal penalties, and operational disruptions. The purpose of this policy is to help protect SnowBe Online, its employees, visitors, and vendors. Ensuring the proper authentication and access for SnowBe Online.

Account Management - #009 (AC#2)

- The purpose of this policy is to establish a standard for creating, managing, using, and removing accounts that provide access to SnowBe Online's information systems or technology. Each account must include a user ID and a password. Providing these account credentials grants access to company services and resources. This policy outlines the rules for issuing and managing accounts.

Privileged Access - #010 (AC#6)

- The purpose of this policy is to establish protocols for managing Privileged Access to IT Resources, ensuring adherence to the Principle of Least Privilege, and promoting transparency, accountability, and security across SnowBe Online through thorough documentation, review, and auditing of access requests.

Change Control Management - #011

- The purpose of this policy is to establish a consistent process for requesting, reviewing, approving, and documenting configuration and system changes at the SnowBe company. This ensures that all modifications are properly evaluated to maintain system integrity, availability, and confidentiality of SnowBe's data and services. Ultimately, this policy supports SnowBe's goal of protecting Confidentiality, Integrity, and Availability across all information systems and locations.

Device Lock and Session Termination - #012 (AC#11&12)

- The Device Lock and Session Termination Policy helps SnowBe Online protect sensitive company and customer information by automatically locking or ending inactive sessions. This control reduces the risk of unauthorized access to systems and data across all company devices, whether in the Los Angeles office, retail stores, or through remote VPN connections. By enforcing secure session management, SnowBe strengthens its cybersecurity posture, supports PCI compliance, and ensures the protection of both business and customer trust.

Information Flow Enforcement - #013 (AC#4)

- The Information Flow Enforcement Policy ensures that SnowBe Online controls how information moves within and between its systems. By managing data flow across internal networks, cloud servers, and retail locations, this control helps prevent unauthorized data sharing or exposure. Implementing this policy protects customer information, supports PCI compliance, and maintains the integrity of SnowBe's business operations as the company continues to grow both online and internationally.

Information Sharing - #014 (AC#21)

- The Information Sharing Policy establishes how SnowBe Online securely shares information within the company and with external partners, vendors, and customers. This control ensures that only authorized data is shared through approved channels, reducing the risk of data leaks or unauthorized disclosures. By implementing clear information-sharing standards, SnowBe protects customer privacy, maintains compliance with industry regulations, and supports trusted collaboration across its global operations.

Standards and Procedures

New Account Management Procedures - #001

- This procedure provides guidance and direction regarding the granting, maintenance, and removal of access to the information technology assets of SnowBe Online. IT Assets must be protected by controls to ensure that only those persons with a legitimate need to access IT Assets have access, and that the level of access is appropriate to each person's job duties.

Password Procedures - #002

- The Password Procedures outline the steps SnowBe Online employees must follow to create, manage, and protect passwords used to access company systems, applications, and data. These procedures ensure that all user accounts are secured with strong, unique passwords that meet company security requirements. By following this process, SnowBe reduces the risk of unauthorized access, data breaches, and identity misuse while maintaining compliance with PCI DSS and other cybersecurity standards.

Password Standard - #003

- This standard establishes the baseline security requirements for creating and managing passwords across SnowBe Online's systems and applications. It promotes consistency in password strength and protection

practices, reducing the risk of unauthorized access to company and sensitive customer data. By defining clear password requirements, SnowBe strengthens its overall access control framework and supports compliance with PCI DSS and other industry security standards.

Exceptions/Exemptions

Requests for an exception must be submitted in writing to the IT Director or IT Manager and include details such as the length of time requested, the specific policy or standard involved, and the reason for the request. The IT Director or IT Manager will review each submission to determine whether the exemption is justified and whether compensating controls are required. If the non-compliance results from an improved or alternate solution, an exception is still required and will be formally evaluated and approved prior to implementation. Exemptions include Access Control functions such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies which may not be paused, disabled, or discontinued under any circumstances.

Version History Table

Version	**Date**	**Description**
1.0	10-2-25	Initial draft of the Security Plan
1.1	10-5-25	Feedback inspired template
2.0	10-13-25	Updated Definitions and Policies
3.0	10-20-25	Corrected format and font; Added policies and procedures
4.0	10-23-25	Corrected spacing, fonts, format

Citations

Miya Ferguson

Nevada State University – Used for Scope - https://nevadastate.edu/wp-content/uploads/2025/05/5.1.2-Information-Security-Plan.pdf

Howard University – Used for Scope - https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf

Devin J. Jimenez

University of Arizona – Used for Introduction - https://policy.arizona.edu/information-technology/information-security-program-policy

State of Hawaii Department of Law Enforcement – Used for Definitions - https://law.hawaii.gov/wp-content/uploads/2023/12/ADM.09X.30.pdf

Sean Redding

Fordham University/Michigan University – Used for Roles and Responsibilities / Exceptions & Exemptions- https://it.uw.edu/wp-content/uploads/2024/08/Information_Security_Guideline.pdf

Fordham University - Used for Roles and Responsibilities / Exceptions & Exemptions - https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/web-application-security-polic

PCI DSS – For Requirements - https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf