SNOWBE ONLINE SECURITY PLAN

Group Member Names:
Jeremy Sarduy
Travis Ferrufino
Vanessa Campbell
Eddy Cruz
David Perez Puello

Table of Contents

Section 1: Introduction ***2***

Section 2: Scope ***2***

Section 4: Roles & Responsibilities ***3***

Section 5: Statement of Policies, Standards and Procedures ***3***

Policies **4**

Section 6: Exceptions/Exemptions ***7***

Section 7: Version History Table ***8***

Citations ***8***

Section 1: Introduction
To enhance the security of SnowBe Online's data and information systems, there is a need to establish consistent and repeatable information security practices. It is crucial to identify the roles responsible for developing, approving, and implementing these practices to ensure a robust security framework.

Section 2: Scope
The SnowBe Online Security Plan aims to establish and maintain a robust security framework encompassing all facets of the organization's operations. This scope outlines the specific areas and components that will be addressed to safeguard information systems, data, and customer assets. The scope of work highlights and prioritizes the different stakeholders operating customer data and information systems as it is transmitted throughout the network, from Representative's managing the initial transactions to IT professionals managing the data once received.

Section 3: Definitions
Access Control

- Mechanisms that manage who can enter or use SnowBe Online's physical resources.

Behavioral Analysis

- A security approach that analyzes patterns of behavior to detect and prevent potential threats.

Compliance

- Adherence to company policies, legal standards, and regulatory requirements.

Criticality

- The level of importance assigned to a vulnerabilities or patch based on the potential impact and urgency.

Endpoint and Responses (EDR)

- A security solution providing real-time monitoring and response capabilities to potential security at the endpoint level.

Incident

- An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

Incident Response Team (IRT)

- The group is responsible for managing and coordinating responses to security incidents.

Least Privileges Principle

- Users granted only the access necessary for their specific job functions.

Maturity Model

- A framework that provides a structured approach to assessing and improving the cybersecurity capabilities and processes of an organization.

Physical Asset

- Any property owned by SnowBe Online, including buildings, hardware, and infrastructure.

Patch
- Software or system updates provided by stakeholders to fix security vulnerabilities or other issues.

Role-Based Access Control (RBAC)
- Access privileges assigned based on job responsibilities and roles.

Risk Assessment
- The process of identifying, evaluating, and mitigating risks to Snowbe and their information systems.

Surveillance Systems
- Cameras and related technology used for monitoring premises.

System Development Life Cycle (SDLC)
- Process used by Snowbe to design, develop, test, and deploy systems and applications, ensuring that they meet business and security requirements provided by the company.

Security Requirements
- Specific measures and controls implemented during the SDLC phases to protect the system and its data from unauthorized access, modification, or destruction.

Vulnerability
- A flaw or weakness in a system that can be exploited to compromise security.

Zero-Day
- A vulnerability that is exploited by attackers before it is known to the vendor or the public.

Section 4: Roles & Responsibilities
Chief Information Security Officer (CISO):
- Responsibility: Develop, annually review, update, and implement SnowBe's information security plan.

Director/Manager of IT in Each Unit:
- Responsibility: Develop, annually review, update, and implement the information security plan for their respective unit.

Employees:
- Must comply with all physical security procedures and report any security incidents or vulnerabilities.

Facilities Management:
- Responsible for maintaining secure and safe physical working environments.

Senior Leadership for Each Unit at UF:
- Responsibility: Review and approve the information security plan for their unit, including updates as necessary.

Section 5: Statement of Policies, Standards and Procedures

Policies
Incident Response Policy – SP – 1

Physical Security Policy – SP – 2

Data Access Control Policy – SP – 3

Anti-Virus and Backup Policy – SP – 4

Security Training and Awareness Policy SP – 5

- Purpose: Security Awareness and Training Policy establishes the requirements to assist Information Technology (IT) system managers, administrators, and users of SnowBe systems and data the steps to ensure that the systems and data are appropriately safeguarded.

Auditing Policy SP – 6

- Purpose: This Policy is to advise the users of security scanning procedures and precautions used by SnowBe to audit their network and systems. Other persons or entities, unless authorized, are prohibited from performing any such audits.

Remote Access Policy SP – 7

- Purpose: To establish and create guidelines and procedures for secure and authorized remote access to networks, systems and data. To ensure remote connections adhere to security standards, confidentiality, integrity, and availability of sensitive materials and data.

Vendor Management Policy SP – 8

- Purpose: Is the process and standards for engaging and overseeing third-party vendors, suppliers, or service providers to SnowBe. The purpose is to mitigate risk associated with outsourcing applications and resources by creating clear expectations, accountability, and security measures.

Software Development Life Cycle SP – 9

- Purpose: This policy is to establish a comprehensive framework for development, implementation, and maintenance of information systems within Snowbe. This policy aims to ensure that security measures are integrated throughout the System Development Life Cycle (SDLC), protecting both company data and systems.

Software Patch Management Policy SP – 10

- Purpose: The purpose of this policy is to ensure that all SnowBe Online Owned devices are proactively managed and patched with appropriate security updates. In addition, this policy is intended to instruct and inform SnowBe employees and end users, about the change in end-point computing.

Security Maturity Policy SP – 11

- Purpose: Is to provide a structure for SnowBe Online to baseline current capabilities in cybersecurity while establishing a foundation for consistent evaluation. By implementing a cybersecurity maturity model, SnowBe will not only have a framework for measuring the maturity of their cybersecurity

program, but also guidance on how to reach the next level as SnowBe's maturity grows and continues to change.

Access Control Policies

AC-1 – Policy and Procedures

Purpose: To establish a formal framework for managing and securing information systems and data. Policies and procedures provide clear guidelines for employees, ensuring consistency in security practices and compliance with regulatory requirements.

AC-2 – Account Management

Purpose: To ensure that user accounts are created, maintained, and terminated in a secure and controlled manner. Account management aims to prevent unauthorized access, protect sensitive information, and maintain the integrity of the system.

AC-3 – Access Enforcement

- Purpose: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-4 – Information Flow Enforcement

- Purpose: Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization – defined information flow control policies.

AC-7 – Unsuccessful Logon Attempts

- Purpose: Limit the number of consecutive invalid login attempts by a user within a specified time. Automatically take predefined actions (such as locking the account, delaying the next login prompt, notifying the administrator, or other specified actions) when the maximum number of unsuccessful login attempts is reached.

AC-10 – Concurrent Session Control

AC-11 – Session Lock

- Purpose: To establish guidelines for automatic session lock mechanisms to enhance information systems security by preventing unauthorized access without active user participation.

AC-11 – Device Lock

- Purpose: To ramp up system security, it's a good move to have the device locked kick in on its own after a set inactive stretch. Plus, make it a rule for users to hit the lock button before stepping away from the system. Keep that lock intact until the user logs back in using the usual ID and authentication steps. This helps tighten up access control and overall system security.

AC-12 Session Termination

Purpose: To protect against unauthorized access and data breaches by automatically terminating inactive or idle sessions. Session termination ensures that unattended sessions do not pose a security risk, reducing the likelihood of unauthorized actions or data exposure.

AC-17 – Remote Access

- Purpose: Manage and regulate user sessions within a computer system or structured application. This would involve user logins, monitoring session activities while ensuring efficient user interactions between sessions.

AC-18 – Wireless Access

- Purpose: Allowing users to connect to a network or computer system from a distant location utilizing flexible work arrangements, supporting remote teams, and facilitating efficient collaboration. Ensuring a secure connection, providing employees, customers, partners, or clients with the ability to access data and resources remotely.

AC-19 Access Control for Mobile Devices

Purpose: To safeguard sensitive information and maintain system security by enforcing access on mobile devices. This includes implementing measures such as authentication, encryption, and remote wipe capabilities to prevent unauthorized access and data loss in case of device theft or loss.

AC-34 Identity and Access Management Policy

- Purpose: this policy is to define required access control measures to all SnowBe systems and applications to protect the privacy, security, and confidentiality of SnowBe information technology resources

AC-35 – Access control Audit

- Purpose: Regular operational, process, and security audits help to ensure that proper controls are sufficient and effective at providing information confidentiality, protecting Personally Identifiable Information (PII), ensuring system availability, and fostering a higher degree of data integrity. This policy sets forth SnowBe's practice regarding SnowBe information system related audits.

Standards and Procedures
Cryptography and Encryption Control Policies
SC-10 – Network Disconnect

- Purpose: Creating terminating network connections associated with communications sessions or de-allocating networking assignments at the application level if multiple application sessions are a single, operating system-level network connection.

SC-17 - Public Key Infrastructure Certificates

- Purpose: Establish the responsibilities and measures for the implementation and usage of Public Key Infrastructure (PKI) Certification Authority (CA) by SnowBe.

SC-23 – Session Authenticity

- Purpose: Addresses communication protections at the session, versus at packet level and establishes grounds for confidence at both ends of communications sessions.

SC-30 – Concealment and Misdirection

- Purpose: Employ the following concealment and misdirection techniques for SnowBe to confuse and mislead adversaries

Passwords standards

- The parameters in this policy are designed to comply with relevant legal and regulatory standards, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Password Procedure

- This procedure is to communicate the standards for strong passwords, their protection and the frequency of change.

Section 6: Exceptions/Exemptions
How to Request:

Submit a formal written request to the Chief Information Security Officer (CISO) using the designated exception/exemption request form available on the SnowBe Online portal.

Why it is Being Requested:

Provide a detailed justification explaining the necessity for the exception/exemption, including any mitigating controls in place to address potential risks.

Who Can Approve:

Approval authority rests with the CISO, who will assess the request based on its merits and alignment with SnowBe Online's overall security objectives.

How Long the Exception/Exemption Will be in Place:

Clearly specify the duration for which the exception/exemption is sought, outlining any conditions for renewal or termination. Where none are given a limit of one month will be the default.

Section 7: Version History Table

Version	Date	Description
1.0	7/28/2024	Snowbe Security Policy

Citations

Data Access Control -What is the Purpose of a Data Access Control Policy? - Satori (satoricyber.com)

Remote Access Policy - https://reciprocity.com/resources/why-are-remote-access-policies-important/ , https://www.strongdm.com/blog/remote-access-policy

Access Controls Listing - https://www.stigviewer.com/controls/800-53, AC: Access Control - CSF Tools

Password Standards - https://blog.netwrix.com/2022/11/14/nist-password-guidelines/