SNOWBE ONLINE SECURITY PLAN

Group Member Names:

Humberto Gonzalez

Version # 4.0
Date: July 26, 2024

Table of Contents

Section 1: Introduction

This security plan provides a comprehensive framework for protecting SnowBe Online's information assets, including data availability, confidentiality, and integrity. It is intended to protect client data, secure online transactions, and assure compliance with all applicable regulations. SnowBe Online's dedication to strong information security is reflected in its Information Security Program (ISP), strict Confidentiality Policy, eCommerce Policy and Practices for online transactions, and Computing Resources, Network, and E-mail Use Policy. Together, these policies provide a secure environment for the company's operations and user data.

Section 2: Scope

This security plan applies to all employees, contractors, and third-party entities associated with SnowBe Online. It includes the protection of all digital and physical assets, such as the online sales platform hosted on AWS, company databases storing customer information and purchase history, multiple storefronts in the United States and Europe, desktop and laptop computers used in the Los Angeles main office, and on-premise and AWS servers that manage various business functions. This plan addresses all areas of the company's activities, ensuring that comprehensive security measures are in place throughout all sites and systems.

Section 3: Definitions

N/A

Section 4: Roles & Responsibilities

Employees: SnowBe Online employees must adhere to security policies and procedures. Employees should actively participate in security awareness training, and promptly report any security concerns

IT Department: The IT Department at SnowBe Online oversees the technical aspect of the security program and is responsible for implementing, maintaining, and continuously improving security controls per the NIST 800-53. They harden systems, manage patches, secure networks, and protect data through encryption and backups.

Senior Management/Executive Team: The senior leadership at SnowBe Online serves as the authority for information security, setting the tone and direction for the entire organization. They are responsible for establishing and ensuring that resources are allocated to protect SnowBe Online's information assets.

Third-Party Vendors: Vendors will comply with SnowBe Online security requirements. Vendors need to ensure the security of data and systems that interact with SnowBe Online are complying with SnowBe's security requirements.

Section 5: Statement of Policies, Standards and Procedures

Policies

AC-3 Access Enforcement- The purpose of this policy is to ensure that access to SnowBe Online's information systems and data is strictly enforced by existing security standards. This policy is intended to prevent unwanted access, safeguard sensitive information, and guarantee that all access is properly regulated and monitored.

AC-2 Account Management- This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at SnowBe, including all personnel affiliated with third parties with authorized access to any SnowBe information system.

CM-3 Change Control Management Policy- Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.

CEK-03 Data Encryption Policy- The purpose of an encryption policy is to establish, at a senior management level, the business and compliance expectations that the organization needs to meet.

SI-7 Endpoint Security Policy- Enables the protection of devices that employees use for work purposes or servers that are either on a network or in the cloud from cyber threats.

IR-1 Incident Response- This policy establishes a structured and efficient process for managing security incidents, minimizing their impact on SnowBe Online's operations, customers, and reputation.

AC-6 Least Privilege- This policy is intended to guarantee that SnowBe Online workers, contractors, and third-party entities have access to only the information and resources required for their specialized tasks. This policy attempts to minimize the possibility of unauthorized access or data breaches by implementing the principle of least privilege.

AC-19 Mobile Device Policy- The purpose of this policy is to establish the procedures and protocols for the use of mobile devices and their connection to the network.

CA-9 Network Security Policy- A network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization’s network security environment and defines how the security policies are implemented throughout the network architecture.

AC-1 PCI Policy- This policy provides guidance about the importance of protecting payment card data and customer information. Failure to protect this information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of SnowBe Online.

PE-1 Physical Security Policy- The purpose of the Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to SnowBe's Information Resource facilities.

AC-15 Privacy Policy- This Privacy Policy outlines how we collect, use, disclose, and safeguard your personal information when you use our website, mobile applications, or interact with our services. We are committed to complying with applicable data protection laws and regulations.

AC-17 Remote Access- The purpose of this policy is to define rules and requirements for connecting to SnowBe Online's network from any host. These rules and requirements are designed to minimize the potential exposure to SnowBe Online from damages which may result from unauthorized use of SnowBe Online resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical SnowBe Online internal systems, and fines or other financial liabilities incurred as a result of those losses.

AC-16 Security and Privacy Attributes- This NIST control mandates that organizations establish, allocate and uphold security attributes to guarantee access control and compliance with security protocols.

AT-2 Security Awareness Training Policy- Security awareness training helps prevent and mitigate human risk. Designed to help users understand the role they play in combatting security breaches, effective security awareness training teaches proper cyber hygiene, security risks, and how to identify cyber-attacks delivered via email and web browsing.

AC-5 Separation of Duties- Segregation of Duties (SoD) is put in place to lower the chances of mistakes and fraudulent activities by distributing tasks among people guaranteeing that one individual does not have authority over all parts of important business procedures. This establishes a framework for oversight strengthens controls and boosts responsibility within the company.

AC-12 Session Termination- Session termination is an important part of the session lifecycle. Reducing to a minimum the lifetime of the session tokens decreases the likelihood of a successful session hijacking attack.

SI-7 Software, Firmware, and Information Integrity- The main goal of SI-7 is to safeguard software, firmware and data integrity by thwarting alterations and guaranteeing the precision and dependability of these elements. This measure aids companies in thwarting identifying and addressing integrity breaches that might jeopardize the safety of their systems and information.

AC-7 Unsuccessful Logon Attempts- Unsuccessful Logon Attempts is a cybersecurity control that helps to protect information systems by limiting the number of unsuccessful logon attempts that a user is allowed to make. This control is important because it can help to prevent unauthorized access to information systems and data.

SC-12 Cryptographic Key Establishment and Management- Maintaining and managing keys is crucial, for SnowBe's security when dealing with credit card information. Effective key management is essential to safeguard transactions and protect customer data.

SC-13 Cryptographic Protection- Ensuring protection is an element in safeguarding the confidentiality and integrity of customer data stored on SnowBe's platforms. This measure also plays a role in securing VPN connections utilized by sales laptops.

SC-28 Protection of Information at Rest- Safeguarding information at rest is of importance for SnowBe given the storage of customer data and purchase history. Implementing this measure will enhance the security of this data against access or breaches.

SI-02 Software Patch Management- This policy establishes software patch management methods to maintain SnowBe Online's system security, functionality, and compliance. It applies to all organizational software and systems, including workstations, servers, and third-party integrations. It emphasizes the rapid discovery, testing, and application of critical and non-critical patches.

CMMC Security Maturity Policy- This policy uses the Cybersecurity Capability Maturity Model (C2M2) to evaluate and improve SnowBe Online's security policies. It establishes maturity levels in essential security domains and promotes ongoing improvement through gap analysis, metrics monitoring, and training. The policy complies with regulations including PCI DSS, GDPR, and CCPA.

SDLC-1 System Development Life Cycle- This policy outlines SnowBe Online's implementation of a Secure Development Life Cycle (SDLC) framework based on NIST SP 800-160 and SSDF recommendations. It ensures secure software development, deployment, and maintenance by including security measures throughout the SDLC process. The policy is applicable to both internal and third-party development initiatives to improve data security, integrity, and compliance with standards such as PCI DSS and NIST 800-53.

Standards and Procedures

SOP-AC-1 New Account Procedure- Establishing a process for setting up and managing user accounts is essential for ensuring security measures are in place.

SOP-PP-1 Password Procedure- Creating a password procedure aims to set out rules and recommendations, for generating, handling and upkeeping passwords to boost security, maintain uniformity, meet standards and guard against entry and data leaks.

SOP-PS-1 Password Standard- The Purpose of this Standard is to assign unique individual logins and demand password security to limit access to SnowBe Online networks, systems, applications, and data. If a password is compromised, an unauthorized user may get inappropriate access.

Section 6: Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Section 7: Version History Table

Version	**Date**	**Description**
V 1.0	07/07/2024	Initial Version
V 2.0	07/14/2024	Policy Additions
V 3.0	07/22/2024	Policy Revision
V 4.0	07/26/2024	Final Revision
V 5.0	11/24/2024	Software Patch Management, CMMC Security Maturity, and SDLC policies added.

Citations

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

Purpose/Introduction- Michigan Technological University Information Security Plan (mtu.edu)

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)

Physical security Policy- Physical Security Policy Template | FRSecure

Network Security Policy- Network security policy examples & procedures | AlgoSec

Security Awareness Policy- What is Security Awareness Training? | Mimecast

Data Encryption Policy- Encryption policy - AWS Prescriptive Guidance (amazon.com)

Endpoint Security Policy- What is Endpoint Security? How Does It Work? | Fortinet

Incident Response Policy- "Computer Security Incident handling Guide," Special Publication 800-61 | PDF (slideshare.net)

Privacy Policy- Privacy Policy – Personal Training Ennis, CO, Clare | Ozone Gym

Remote Work Security Policy- Remote Working Policy & Best Tips for Remote Workers (factorialhr.com)

Remote Access Policy- Remote_Access_Policy.docx (live.com)

Mobile Device Policy- LEP Mobile Device Policy.docx (live.com)

Least Privileged Citations- https://csf.tools/reference/nist-sp-800-53/r5/ac/

Access enforcement- https://fso-lms4-immortal-assets.s3.us-east-1.amazonaws.com/1411/20216/4d126967-102f-4196-9748-1ac7193[…]3D%22NIST.SP.80053r5.pdf%22&x-id=GetObject

Unsuccessful Login Attempts- https://nist-800-171.certificationrequirements.com/toc473014232.html

Segregation of Duties-
http://sceis.sc.gov/documents/Segregation_of_Duties_Policy_User_Group_Slides.pdf
https://www.catalyst.org/wp-content/uploads/2022/01/Segregation-of-Duties-Standard.pdf

Change Management- https://frsecure.com/change-management-policy-template/

CM-03 Configuration Change Control- https://www.opensecurityarchitecture.org/cms/library/08_02_control-catalogue/154-08_02_CM03#:~:text=Configuration%20change%20control%20involves%20the,system%2C%20including%20up grades%20and%20modifications

Password Policy- https://its.weill.cornell.edu/policies/1115-password-policy

SDLC Security- opm.gov/about-us/open-government/digital-government-strategy/fitara/opm-system-development-life-cycle-policy-and-standards/

CMMC Security Maturity- C2M2 Version 2.1 June 2022 | CMMC Resources & Documentation

Patch Management- Patch Management Policy Template