SNOWBE ONLINE SECURITY PLAN

Ydali Hernandez

Version # 1
Date November 23, 2024

Table of Contents

Section 1: Introduction

To establish a structured framework for protecting the integrity, confidentiality, and availability of SnowBe Online's data and information systems. This plan outlines the necessary procedures and responsibilities required to safeguard the company's digital assets against threats and vulnerabilities.

Section 2: Scope

Applies to all employees, contractors, vendors, and any other individuals who access or handle SnowBe Online's information systems and data. It covers all devices, network components, and systems, including but not limited to desktops, laptops, servers, mobile devices, and cloud services.

Section 3: Definitions

Access Control Control Family:
Refers to a set of guidelines and best practices defined by the National Institute of Standards and Technology (NIST) Special Publication for managing and enforcing access control policies and procedures.
Availability:
Assurance that information and resources are accessible to authorized users when needed.
Backup solutions:
Methods and systems used to create and store copies of data to protect against loss or corruption.
Chief Information Officer (CIO):
The executive responsible for the management, implementation, and usability of information and computer technologies.
Compliance Audit:
A systematic review of security practices and policies to ensure adherence to regulatory and organizational standards.
Compliance Officer:
An individual responsible for ensuring that the company complies with external regulations and internal policies.
Confidentiality:
Assurance that sensitive information is accessed only by authorized individuals.
Critical Patch:
A security update that addresses unknown vulnerability with a higher risk of exploitation.
Cyber Threats:
Potential malicious attempts to damage or disrupt a computer network or system, including malware, phishing, ransomware, and other forms of cyber-attacks.
Data Breaches:
Incidents where confidential, sensitive, or protected data is accessed, disclosed, or stolen by unauthorized individuals.
Data Integrity:
The accuracy, consistency, and reliability of data throughout its lifecycle. It ensures that data remains unchanged and unaltered during storage, transfer, and retrieval, except by authorized actions.
Integrity:
Assurance that the information is trustworthy and accurate.
Network Infrastructure:
The hardware and software resources of a network that enable network connectivity, communication,

operations, and management of an enterprise network. This includes the internet, intranet, and any cloud-based services used by SnowBe.

Operating System Updates:
Software updates that fix vulnerabilities and improve the functionality and security of an operating system.

Patch:
A software update designed to fix vulnerabilities, improve performance, or add features.

Patch Management:
The process of applying updates to software and hardware to address vulnerabilities.

PCI DSS:
Payment Card Industry Data Security Standard, a set of security protocols for handling card transactions.

Principle of Least Privilege:
A security concept where users are granted the minimum levels of access- or permissions -needed to perform their job functions.

Role-based Access Control:
A method of regulating access to computer or network resources based on the roles of individual users within an organization.

Security Incident:
Any event that threatens the integrity, confidentiality, or availability of information systems or data.

Security Maturity:
The organization's ability to protect its assets, respond to threats, and continuously improve security practices based on a structured framework like NIST 800-53 or CMMC.

Separation of Duties:
A security concept that prevents conflict of interest by dividing tasks and privileges among multiple people or systems.

Threat Monitoring:
The ongoing process of detecting and analyzing potential security risks to the organization.

User Account:
A unique identifier assigned to an individual or system for accessing SnowBe Online's systems and data.

VPN:
Virtual Private Network used for secure remote access.

Section 4: Roles & Responsibilities

Administrators:
Implement and maintain access control mechanisms in line with the policy.
Ensure the secure creation, modification, and deletion of user accounts.
Report any security incidents or policy violations to senior management.

Chief Information Officer (CIO):
Develops and oversees the implementation of the security policy.
Approves network extensions and significant security measures.

Compliance Officer:
Ensures the company meets regulatory requirements.
Conducts regular audits and assessments of the security controls.

Employees:
Follow access control policies and procedures.
Participate in security training and awareness programs.
Report any suspicious activity or security incidents.

Use strong passwords and secure authentication methods.
Protect sensitive information and comply with data protection policies.

IT Department:

Ensures all network devices are updated and patched regularly.
Maintains antivirus and backup solutions.
Manage access controls and monitors network activity.
Responds to security incidents and ensures compromised devices are secured.

Senior Management:

Ensure that the security policy is enforced across all departments and locations.
Assess and manage risks associated with data and system access.
Ensure that appropriate measures are in place to mitigate identified risks.
Ensure compliance with relevant laws, regulations, and industry standards.

Third-Party Vendors:

Ensure their products and services meet SnowBe's security requirements.
Cooperate with SnowBe during security assessments and audits.
Implement and maintain appropriate security measures.
Notify SnowBe of any security incidents or breaches that may affect the company's information assets.
Sign confidentiality agreements and adhere to data protections standards.

Section 5: Statement of Policies, Standards and Procedures

Policies

Access Control-009

The purpose of this policy is to define the SnowBe policy and procedures for implementing and maintaining appropriate access controls for SnowBe information assets. This document corresponds to the Access Control Control Family of National Institute of standards and technology special Publication.

Account Management-2

The purpose of this policy is to ensure the secure management of user accounts, access controls, and related security measures for SnowBe Online. This policy aims to maintain the integrity, confidentiality, and availability of SnowBe's systems and data. By establishing standardized procedures for account creation, control, and monitoring, we aim to protect customer and business information across all platforms and devices used by the company.

Change Control Management-1

The objective of Change Management at SnowBe is to ensure that standardized methods and procedures are utilized to enable beneficial changes while ensuring efficient and prompt handling of all modifications to services provided by SnowBe's technical infrastructure. The primary goals of Change Management are to minimize the disruption of services, reduce back-out activities, and ensure clear communication across IT and its customers.

Employee Training and Awareness Policy-1

This policy will mandate periodic cybersecurity training sessions covering topics such as identifying phishing attempts, using secure passwords, and understanding data privacy regulations. It will also include simulated phishing exercises to test and improve employee awareness.

Least Privilege-6

The purpose of this policy is to ensure the security of SnowBe Online's data and systems by implementing the principle of least privilege and separation of duties. This policy outlines the responsibilities of employees and administrators in maintaining secure access to data and services.

Network Security Policy-1

This policy will include guidelines on using firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). It would also cover secure configuration measures for network devices, regular monitoring of network traffic, and protocols for responding to network threats.

Network Security Policy-009

The purpose of this policy is to establish a comprehensive framework for protecting the network infrastructure and data integrity of SnowBe Online. This includes safeguarding the online sales platform, in-store systems, customer information, and all other digital assets from unauthorized access, cyber threats, and data breaches. By implementing this policy, SnowBe Online aims to ensure the confidentiality, integrity, and availability of its information systems, thereby maintaining customer trust and compliance with relevant legal and regulatory requirements.

Security Maturity Policy-1

The purpose of this policy is to enhance SnowBe Online's security posture by adopting industry-recognized frameworks, continuously improving processes, and fostering a culture of proactive risk management and compliance.

SnowBe Online Payment Card Industry-009

The purpose of this policy is to establish a framework for the protection of payment card data and customer information in accordance with the Payment Card Industry Data Security Standard (PCI DSS) v3.2. SnowBe Online is committed to maintaining the highest level of security for cardholder data to prevent data breaches, financial loss, and damage to the company's reputation. This policy outlines the necessary security measures and procedures to ensure compliance with PCI DSS requirements.

System and Software Patch Management Policy-1

The purpose of this policy is to ensure that all systems and software at SnowBe Online are updated regularly to address vulnerabilities, improve performance, and maintain compliance with security standards.

System Development Life Cycle policy-1

The purpose of this policy is to integrate security measures into every phase of the System Development Life Cycle (SLDC), ensuring that systems and applications are developed, implemented, and maintained with a strong security foundation.

Standards and Procedures

New Account Procedure-1

The purpose of this procedure is to establish a standard for the administration of computing accounts that facilitate access or changes to SnowBe Online's information resources. An account, at minimum, consists of a user ID and a password. Supplying account information will usually grant access to some set of services and resources. This policy establishes guidelines for issuing and managing accounts.

Password Procedure-1

Passwords are a crucial aspect of computer security, serving as the frontline defense for user accounts. The purpose of this procedure is to establish a standard for creating strong passwords, protecting them, and changing them regularly to enhance the security of SnowBe Online's systems and data.

Password Standard-1

The purpose of this password standard is to ensure the security of SnowBe Online's information systems by enforcing robust password management practices. This standard aims to protect user accounts and sensitive data from unauthorized access and potential security breaches.

Section 6: Exceptions/Exemptions

To request an exception or exemption the individual must submit a request to the department manager, who then will forward it to the IT department manager. The request must include a detailed explanation of the necessity for the exception or exemption, covering the business or technical reasons that justify the deviation from the standard policy.
The IT Manager will review the request to ensure all required information is provided and will assess the potential security impact. A formal risk assessment will be conducted to evaluate the implications of the requested exception or exemption.
The IT Manager will then either approve or deny the request. The duration for the exception or exemption will be 18 months unless the requester specifies otherwise. Additionally, the exception or exemption will be subject to periodic reviews to ensure it remains necessary and that security risks are adequately managed.

Section 7: Version History Table

Version	Date	Description
1	07/05/2024	Initial draft
2	07/11/2024	Added policies: Employee Training and Awareness Policy, Network Security Policy, Least Privilege, Account Management.
3	07/21/2024	Added Policies: Change Control Management, New Account Procedure.
4	07/27/2024	Changed New Account Procedure from policy to procedure. Added Password Standard and Password Procedure.
5	11/22/2024	Added Policies: System Development Life Cycle policy, System and Software Patch Management Policy, and Security Maturity Policy.

Citations

Associate Vice President for Technology Resources (2021, August 17). *System Development Life Cycle (SDLC) Methodology and Project Management Practices*. Texas State. Retrieved November 22, 2024, from https://policies.txst.edu/university-policies/04-02-03.html

AVP Information Technology (2011, October 28). *UB Network Connection Policy*. University at Buffalo. Retrieved July 5, 2024, from https://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/ub-network-connection.html

Chief Information Security Officer (2022, December 16). *CYBERSECURITY MATURITY MODEL CERTIFICATION STANDARD V2.0 LEVEL 2*. University System of New Hampshire. Retrieved November 22, 2024, from https://www.usnh.edu/it/sites/default/files/media/2022-12/cmmc_v2level2-std-12122022.pdf

Information Technology (n.d.). *Account Management*. Montclair State University. Retrieved July 20, 2024, from https://www.montclair.edu/policies/all-policies/account-management-policy/

Jill, S. (n.d.). *Account and Identity Management Policy*. Colorado Department of Education. Retrieved July 11, 2024, from Account and Identity Management Policy

Michigan Tech (2011, October 13). *Information Security Plan*. Michigan Technological University. Retrieved July 5, 2024, from https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

NIST (n.d.). *Security and Privacy Controls for Information Systems and Organizations*. DOI. Retrieved July 11, 2024, from NIST Security and Privacy Controls for Information Systems and Organizations

Office of Technology Services (n.d.). *Change Management Policy*. Louisiana Division of Administration. Retrieved July 20, 2024, from https://www.doa.la.gov/media/lhibcody/ots_change_management_policy.pdf

Office of the Vice President for University Operations (n.d.). *Patch Management Policy*. University of Portland. Retrieved November 22, 2024, from https://www.up.edu/is/files/policy-patchmanagement.pdf

SEMO (n.d.). *Least Privilege Policy*. Southeast Missouri State University. Retrieved July 11, 2024, from https://semo.edu/finance-admin/_pdfs/10-15-policy-least-privilege-policy-v8-ready.pdf

University of Colorado (n.d.). *IT Security Program*. Retrieved July 5, 2024, from https://www.cu.edu/ope/aps/6005