SNOWBE ONLINE SECURITY PLAN

Daphnie Bruno

Version # 1.0
Date: March 24, 2025

Table of Contents

Section 1: Introduction *2*

Section 2: Scope..................... *2*

Section 3: Definitions..................... *3*

Section 4: Roles & Responsibilities *16*

Section 5: Statement of Policies, Standards, and Procedures *18*

Policies 18

Standards and Procedures 22

Section 6: Exceptions/Exemptions..................... *22*

Section 7: Version History Table *24*

Citations *25*

Section 1: Introduction

The IT Security Plan for SnowBe Online ensures data confidentiality, integrity, and availability while defining, developing, and documenting information security policies and procedures that support business goals and fulfill legal and ethical responsibilities regarding IT resources. These policies serve as foundational guidelines for managing and implementing security measures throughout the organization, establishing a framework of internal controls designed to identify irregularities, prevent waste, fraud, and abuse, and assist in resolving operational discrepancies. When applied consistently, these policies protect IT resources from various threats, ensuring business continuity and maximizing return on investments. The plan reflects SnowBe Online's commitment to safeguarding sensitive customer information and critical business data while recognizing the numerous threats to information security. It stresses the need for customer data privacy protection and adherence to legislation. IT Security Plan also considers PCI-DSS standards regarding the security of cardholder data protection and integrates controls from NIST 800-53 into the approach toward information security management. The plan is reviewed and updated quarterly as SnowBe Online continues to scale its operations, especially given its laid-back culture and increased cyber threats in today’s business environment.

Section 2: Scope

Scope of the Security and Compliance Plan for SnowBe Online

This plan applies to all digital and physical assets, personnel, and customer data involved in SnowBe Online operations in the U.S. and internationally.

Specifically, it covers:

- **Digital Infrastructure**: AWS-hosted website, on-premises servers, digital sales platforms, and data storage systems.
- **Personnel**: All employees, contractors, and consultants accessing company networks, systems, or customer data.
- **Customer Data**: Handling, storage, and protection of sensitive customer information, including credit card details and purchase history.
- **Physical Assets**: Desktops, laptops, and servers at the main office, with access control and security.
- **Compliance Frameworks**: Adherence to NIST 800-53, PCI DSS, and GDPR as relevant.

This scope ensures consistent security and compliance across all relevant areas of SnowBe Online operations.

Section 3: Definitions

The following definitions apply to terms used throughout this security plan. A clear understanding of these terms is essential for adequately implementing and interpreting the security measures described herein.

Access:

The ability to use, modify, or manipulate an information resource or to gain entry to a physical area or location.

Access Control:

The practice of limiting and controlling access to systems and data based on users' roles and responsibilities within an organization. Security measures or policies designed to manage who can view, use, or alter resources within an information system or network.

Access Management:

Defining and controlling who can access specific resources within an organization ensures that only authorized users have the appropriate permissions to use the network and its resources.

Account:

Any combination of a User ID (sometimes referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

Active Directory (AD):

A directory service used for account management and authentication of internal user accounts.

Adherence:

The act of following or sticking to a rule, policy, or principle.

Agency Data Custodian:

An agency official who, based on his or her position, is a fiduciary owner of specific agency information assets. For instance, the Labor Bureau of Unemployment Compensation Director (or designee) is the Agency Data. Custodian for Unemployment Compensation Information Assets and the Department of Health and Human The Services Office of Family Independence Director (or designee) is the Agency Data Custodian for Benefits Information Assets.

Anomalous Accounts:

Accounts that exhibit unusual or unexpected behavior, such as irregular access patterns or unexpected changes, which may indicate potential security risks.

Antivirus Software:

A program designed to detect, prevent, and remove malware and other malicious software from computers and networks, providing ongoing protection against cyber threats.

Attribute-Based Access Control:

An access control method that grants or denies access to resources based on user attributes (e.g., role, location, or department) rather than solely on the user's identity.

Atypical Usage:

Unusual or out-of-the-ordinary behavior in system account usage, such as logging in at odd hours or from unusual locations, which may suggest security concerns or unauthorized

Authentication:

The Process of verifying the identity of a user or device.

Authorization:

The process of obtaining approval for account creation. Also, it could be used to refer to when user obtains permission.

Authorized Change Windows:

Predetermined time periods during which approved changes can be implemented with minimal

impact on operations

Authorized Use:

Use of internal or external systems that is approved and complies with this policy.

Authorized User:

A person with an approved user id and password, able to access the company's network and systems.

Automated Mechanisms:

Tools or systems that perform tasks automatically, often without direct human intervention, to streamline processes such as account creation, modification, and deletion access.

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.

Baseline Security Practices

Minimum security controls that must be implemented to ensure fundamental protection of IT systems.

Business Associate Agreement:

A business Associate Agreement is typically a HIPAA compliance standard. However, it has uses in the case of PCI. In this instance, it is an agreement that outlines the relationship between SnowBe and the vendor signing. This outlines exceptions, acceptance, and consequences of proper data handling and/or disposal.

Business Continuity:

The ability of an organization to maintain essential functions during and after a disaster or disruption, ensuring that critical operations can continue or be quickly resumed.

Cardholder:

Individual who owns and benefits from the use of a membership card, particularly a payment card.

Cardholder Data (CHD):

Elements of payment card information that must be protected, including primary account number (PAN), cardholder name, expiration date, and the service code.

Cardholder Name:

The name of the individual to whom the card is issued.

CAV2, CVC2, CID, or CVV2 data:

The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

Change Advisory Board (CAB):

A group responsible for reviewing, evaluating, and approving change requests, as well as overseeing their implementation.

Change Control Board:

A group responsible for reviewing and approving changes in an organization's processes or

products

CISO:

A CISO, or chief information security officer, is a senior-level executive who oversees an organization's information, cyber, and technology security. The CISO's responsibilities include developing, implementing, and enforcing security policies to protect critical data.

Cleartext:

Unencrypted data that can be read without any special measures.

Commercial Off-The-Shelf (COTS):

Software or hardware products that are ready-made and available for sale to the general public.

Company Information:

Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of SnowBe Online.

Compensating Controls:

Alternative security measures should be put in place to fulfill the requirements of a security standard when the original controls cannot be implemented due to technical or business constraints.

Complexity:

The state of being intricate or complicated.

Composed:

Made up of various parts or elements.

Compromised:

Weakened or damaged, especially in terms of security or integrity

Confidentiality:

Protection of sensitive information so that it is not disclosed to unauthorized individuals, entities or processes.

Confidentiality Agreement:

A formal agreement in which a party agrees to protect and not disclose sensitive or private information. Often used to maintain the privacy and security of organizational data.

Conform:

To comply with rules, standards, or laws.

Consecutive:

Following one after another in order without interruption.

Continuous Improvement:

A process of regularly evaluating and enhancing security practices to adapt to evolving threats and business needs.

CRM (Customer Relationship Management):

A system or software that manages a company's interactions with current and potential customers, using data analysis to improve business relationships, customer retention, and sales growth.

Cyber Security Events, Incidents, and/or Breaches:

- Event - An exception to the normal operation of IT services, such as outages. Not all events are incidents or breaches.
- Incident - Electronic activities that result in unauthorized access or exposure to SnowBe Online Data, or significant impairment of SnowBe Online IT systems. All incidents start as events.
- Breach - The unauthorized acquisition or unauthorized use of either (a) unencrypted data or (b) encrypted electronic data along with the confidential process or key, that can compromise the security, confidentiality, or integrity of personal information that creates a substantial risk of identity theft or fraud against customers. A good faith but unauthorized acquisition of personal information by SnowBe Online or its employees or agents for the lawful purposes of SnowBe Online is not a breach unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure. The term "breach" does not include disclosure of personal information when the disclosure is required by court order or necessary to comply with state or federal regulations.

Cyber Security Incident Response Plan:

Internal protocol for a team(s) of SnowBe Online staff responsible for response to cyber security incidents.

Cyber Security Posture:

The overall security status of an organization, reflecting its capabilities to protect against, detect, and respond to cyber threats, including policies, controls, and measures in place.

Cyber Threat:

Any potential malicious act that seeks to damage, disrupt, or gain unauthorized access to information systems or data, including malware, phishing attacks, and hacking attempts.

Data Breach:

An incident where unauthorized individuals gain access to sensitive or protected data.

Data Breach Notification:

SnowBe Online’s notification requirements in response to a Cyber Security Incident.

Data Minimization:

The practice of collecting only the necessary information required to fulfill a specific purpose.

Data Retention Schedule:

A policy that defines how long different types of data should be kept and when they should be deleted or archived.

Delegates:

People are authorized to act on behalf of others.

Demilitarized Zone:

A separation of public and private LAN’s.

Disclosure:

The act of revealing or making information known.

Disposal:

CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, and USB storage devices in accordance with the Record Retention and Disposition Policy. The approved PCI DSS disposal methods include cross-cut shredding, incineration, and approved shredding and disposal service.

Dissemination:

This is a higher diction compared to simpler alternatives like "distribution" or "sharing." It is often used in formal documentation.

Due Diligence:

The process of evaluating a vendor’s security practices and financial stability before entering into a formal agreement.

Electronic Resources:

Any electronic asset (including devices and data) owned or handled by SnowBe Online.

Emergency Changes:

Urgent modifications made to resolve critical issues or security vulnerabilities, often implemented immediately and documented retrospectively

Encryption:

Security method that renders data elements unreadable by unauthorized parties.

Entity validation:

The process of confirming the identity or legitimacy of an individual, device, or organization, typically before granting access to resources.

Expiration Date:

The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

Exploitation:

The act of using something in a way that may be considered unfair or unethical.

External Systems:

Any system or services operated by third parties that are accessed or used by SnowBe Online.

Facilitate:

Slightly elevated compared to simpler alternatives like "support" or "enable," though it fits in a professional context.

Firmware:

A specialized type of software that is embedded into hardware devices, providing low-level control for the device's specific functions.

Foreign Remote Access:

A less common, and unusual, variety of Remote Access, where SnowBe Online personnel remotely access SnowBe Online information asset(s) from a location outside the United States, U.S. territories, embassies, or military installations.

Guidance:

This word is slightly more formal than "instructions" or "advice," but it's common in professional documents.

Hardware:

The external and internal devices and equipment within computer systems.

Identification:

The process of providing a unique identifier for a user or device.

Information:

Includes both company and customer information.

Information Assets:

Any data, system, or network resource owned or operated by the organization that holds value and requires protection.

Information Resources:

Are all computer and communication devices and other technologies which access, store or transmit company and customer information.

Information Sharing:

The process of exchanging data between individuals or organizations.

In-State Remote Access:

The more common and default, variety of Remote Access, where State of Maine personnel remotely access State of Maine information asset(s) from a location inside the State of Maine, but outside a State of Maine office location.

Integrity:

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…”

IT Resources

Include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

IT Security Officer (ISO):

The individual is responsible for overseeing the organization's information security strategy, ensuring compliance with security policies, and responding to security incidents.

Least Privilege:

A security principle that restricts access rights for users, accounts, and computing processes to only what is strictly required to complete their assigned tasks.

Level I information

SnowBe Online Information has a high risk of significant financial loss, legal liability, public distrust, or harm if this data is disclosed.

Level II information

SnowBe Online Information with a moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, public distrust, or harm if this data is disclosed.

Level III information

SnowBe Online Information with a low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust or harm if this data is disclosed.

Lockout:

A security feature that temporarily disables account access after a specified number of failed logins attempt to prevent unauthorized access.

Long-Term:

30 days or more.

Mac Address:

Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network. SSID Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

Magnetic Stripe (i.e., track) data:

Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

Management:

The group is responsible for supporting and promoting a culture of security awareness within their teams and ensuring that security policies are communicated effectively to all staff.

Maturity Levels

A set of defined stages that measure the effectiveness and sophistication of an organization's security capabilities.

Merchant:

A department or unit (including a group of departments or a subset of a department) approved to accept payment cards and assigned a merchant identification number.

Mitigation Measures:

Actions taken to reduce the severity or impact of potential risks or threats, aimed at minimizing vulnerabilities and enhancing overall security.

Mobile Device:

Any portable device, including laptops, smartphones, or tablets, is used for business operations.

Multi-Factor Authentication (MFA):

A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.

Network Administrators:

The professionals are tasked with ensuring the security and functionality of network devices, including updating firmware and monitoring network traffic for potential breaches or vulnerabilities.

NIST (National Institute of Standards and Technology):

A non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve our quality of life.

Node:

Any device or endpoint within a network that can send, receive, or forward data, such as a computer, server, or router.

On-Premises:

Refers to hardware or software that is physically located within an organization's facilities, as opposed to being hosted in the cloud or managed by a third-party service provider.

Operational Change Management:

A disciplined approach to making alterations to IT systems, services, or processes to maintain quality control and minimize disruption.

Out-of-State Domestic Remote Access:

A less common variety of Remote Access, where SnowBe Online personnel remotely access SnowBe Online information asset(s) from a location outside the SnowBe Online, but within the United States, including U.S. territories, embassies, and military installations.

Oversee:

More formal than "supervise" or "monitor," though common in business settings.

Passphrases:

A sequence of words used for authentication, typically longer than a password.

Patch:

A piece of software designed to update or fix problems with a computer program or its supporting data, addressing security vulnerabilities or improving functionality.

Patch Management Cycle:

A part of lifecycle management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

Payment Card Industry Data Security Standards (PCI DSS):

The security requirements defined by the Payment Card Industry Data Security Standards Council and the major credit card brands including Visa, MasterCard, Discover, American Express, and JCB.

PCI Compliance Committee:

Group composed of representatives from Financial Management, Information Security Office, Office of the Vice President and Chief Information Officer, Internal Audit, and UB merchants.

PCI DSS (Payment Card Industry Data Security Standard):

A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment to protect cardholder data.

Permission:

Is the organizational (Org) unit that is assigned to the Role that will allow the user access to a specific or multiple Org units.

Permitted Actions:

Specific actions or access to resources that are allowed without identification or authentication.

Personal Devices:

Include the following categories:

- Portable cartridge or disk-based, removable storage media (for example, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards or drives that contain nonvolatile memory).
- Portable computing and communication devices with information storage capability (for example, notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

- Any other mobile computing device small enough to be easily carried by an individual, able to transmit or receive information wirelessly, and having local, nonremovable data storage and a self-contained power source.

Personal Information:

Information can be used to identify an individual and/or an individual’s financial account(s), credit history, or credit cards, as well as individual medical records and health plan information. This includes an individual’s social security number, first name (or initial) plus last name, along with his/her driver's license number or state identification card number, financial account number, and/or credit card number.

Personally Identifiable Information (PII):

Information that can be used to identify, locate, or contact an individual, such as name, email address, or credit card details

Personally Owned Resources:

Are information resources under the control of SnowBe Online employees or agents and not wholly owned by SnowBe Online.

Physical Security:

Measures taken to protect physical assets, including buildings, hardware, and other tangible items, from unauthorized access, theft, or damage.

PIN or PIN block:

Personal identification number entered by the cardholder during a card-present transaction or encrypted PIN block present within the transaction message.

Primary Account Number (PAN):

A number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account and includes a check digit as an authentication device.

Principle of Least Privilege:

Access privileges for any user should be limited to resources essential for completion of assigned duties or functions, and nothing more.

Principle of Separation of Duties:

Whenever practical, no one person should be responsible for completing or controlling a task, or set of

tasks, from beginning to end, when it involves the potential for fraud, abuse, or other harm.

Privileged User Accounts:

Accounts with higher-level permissions than standard user accounts, often granting the ability to modify

System settings or access sensitive information.

Provisioning/Deprovisioning:

The processes of creating (provisioning) and removing (de-provisioning) user accounts, resources, or services, especially as individuals join or leave an organization.

Purview:

This word can sometimes be considered higher diction because it's less common in everyday speech, but it's standard in professional contexts.

Regulated Data:

Data that requires SnowBe Online to implement specific privacy and security safeguards as mandated by federal, state, and/or local law, or SnowBe Online policy or agreement.

Removable Media:

Any device with storage capabilities that is also portable. This includes USB thumb drives, portable hard drives, CDs for example

Retention Period:

The amount of time PII is stored before it is deleted or anonymized.

Revocation of privileges:

The act of removing a user's access rights or permissions, usually due to a change in their role or as a response to a security issue.

Risk Assessment:

A process that determines what information technology resources exist that require protection and understands and documents potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Risk-Based Approach

A methodology that prioritizes security improvements based on the likelihood and impact of threats.

Role:

This describes the function a user can perform on the system, e.g. view reports, capture data, create user accounts for specific module on the information system.

Roll-back Plan:

A strategy to revert a system to its previous state in case a change implementation fails or causes unexpected issues.

Runtime Access Control:

A method of managing access to resources dynamically, based on real-time conditions or attributes, allowing permissions to be adjusted instantly without needing to restart sessions.

Sanitization (of computer hard drives):

Removing data on a system through one or more various methods may include overwriting or erasing data utilizing the methods described in NIST Special Publication 800-88.

Screen Lock:

A password-protected mechanism is used to hide data on a visual display while the device continues to operate. Screen locks can be activated manually or in response to rules.

Screen Timeout:

A mechanism that turns off a device display after the device has not been used for a specified time.

Security Administration:

The person charged with monitoring and implementing security controls and procedures for a system. Whereas SnowBe Online may have one Information Security Officer, technical management may designate several security administrators.

Security Breach:

An incident where unauthorized access to data, applications, or networks occurs, potentially leading to the exposure, theft, or destruction of sensitive information.

Security Maturity Model

A structured framework used to assess and improve an organization's cybersecurity posture over time.

Self-Assessment Questionnaire (SAQ):

Validation tools to assist merchants and service providers report the results of their PCI DSS self-assessment.

Sensitive Authentication Data:

Additional elements of payment card information required to be protected but never stored. These include magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN or PIN block.

Sensitive Data:

Any information that requires protection due to its confidential nature, including customer data.

Separation of Duties:

A security principle that divides critical functions among staff members to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud (i.e., no user should be given enough privileges to misuse the system on their own).

Service Code:

Permits where the card is used and for what.

Service Providers:

External organizations or vendors that offer specialized services, such as cloud hosting, data storage, IT support, or software development, to help businesses operate more efficiently.

SnowBe Online affiliates

People and organizations associated with SnowBe Online through some form of formalized agreement.

Software:

The computer programs that run on the devices.

Software Development Life Cycle (SDLC):

The process for planning, creating, testing, and deploying an information system.

Storage:

The method of saving digital information typically involving various media types (e.g., hard drives, cloud storage) that allow data to be retrieved and used when needed.

System Administrators:

The individuals responsible for securing company systems, regularly patching and updating them, and ensuring access control and secure data storage.

Technology Stack:

A combination of technologies used to build and run an application or system, typically including programming languages, frameworks, libraries, servers, and databases.

Third-Party Vendors:

External organizations that provide services to the company and are required to comply with the company's security requirements as outlined in contracts, and attributes, allowing permissions to be adjusted instantly without needing to restart sessions.

Trust Relationships:

Connections or partnerships between entities (e.g., systems, organizations, or individuals) that are built on a basis of mutual reliability, typically to facilitate secure information sharing or system access.

Unauthorized Access:

Access to internal or external systems without proper authorization.

Unsuccessful Logon Attempt:

A failed attempt to log in to a system using incorrect credentials, such as an incorrect password or username.

User:

Anyone with authorized access to the company's business information systems. This includes permanent and temporary employees, third-party personnel such as temporary, contractors, or consultants, and other parties with valid company access accounts.

User ID:

Is a unique identifier assigned to an individual user within a system, application, website, or platform. It is used to differentiate one user from another, allowing the system to track user-specific information, preferences, and activities.

Users of SnowBe Online Data:

Any person extended access and use privileges to SnowBe Online Data. Includes employees, staff, persons hired or retained to perform work for SnowBe Online, and any other person extended access and use privileges by SnowBe Online under contractual agreements or otherwise.

Verification Link:

An email-generated link that a customer will receive to confirm their account during creation.

VPN (Virtual Private Network):

A technology that creates a secure and encrypted connection over a less secure network, such as the Internet, allows users to send and receive data as if their devices were directly connected to a private network.

Voice over Internet Protocol (VoIP):

A technology that allows voice calls to be made using an internet connection instead of a regular phone line.

Vulnerability Analysis:

The systematic examination of systems and applications to identify security weaknesses or vulnerabilities that attackers could exploit.

Vulnerability Management:

The process of identifying, classifying, prioritizing, and remediating vulnerabilities in systems and applications to reduce the risk of exploitation by cyber threats.

WEP:

Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

Wi-Fi:

Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point:

A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC:

A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA:

Stands for Wi-Fi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

Section 4: Roles & Responsibilities

This section explains our organization’s specific roles, responsibilities, and accountability for information security. By clearly defining each individual's and team's duties, we establish a comprehensive framework that ensures effective security governance, risk management, and compliance with our organizational security policies.

Chief Information Security Officer (CISO):

- Oversee all security policies’ overall implementation and enforcement, ensuring alignment with the regulatory framework.
- Report on security incidents and compliance with security policies.

Compliance Officer:

- Ensure SnowBe Online complies with all relevant laws and industry standards, including PCI DSS.

- Work closely with the CISO on audits and risk management.

Employees:

- Adhere to all security policies and procedures.
- Report any suspected security incidents or breaches to the IT Security Officer.

Human Resources (HR):

- Ensure that security awareness training is provided to all employees.
- Support the onboarding and offboarding processes with respect to access controls.

IT Security Manager:

- Conduct day-to-day functions related to security, including maintaining the latest antivirus software.
- Check for any security breaches and patch servers and workstations as needed.

IT Security Officer:

- Manage and coordinate the development and implementation of security policies and procedures.
- Conduct risk assessments and vulnerability analyses.

IT Staff:

- Implement security measures and protocols as defined by the IT security plan.
- Monitor systems for security breaches and respond to incidents.

Management:

- Support and promote a culture of security awareness within their teams.
- Ensure that security policies are communicated effectively to all staff.

Network Administrators:

- Ensure the security and functionality of network devices, including updating firmware.
- Monitor network traffic for potential breaches or vulnerabilities.

System Administrators:

- Secure all company systems, regularly patch and update them.
- Ensure access control and that data is stored securely.

Third-Party Vendors:

- Comply with SnowBe Online's security requirements as outlined in contracts.
- Maintain the security of any data or systems they handle on behalf of SnowBe Online.

Section 5: Statement of Policies, Standards and Procedures

This section outlines the key policies, standards, and procedures governing our organization's information security approach. These guidelines are designed to protect our critical assets, ensure compliance with relevant regulations, and maintain our data's confidentiality, integrity, and availability.

Policies

This section outlines our organization's policies, which serve as the foundational principles guiding our operations and decision-making processes.

AC-01 Policy and Procedures

The purpose of this guide is to provide guidance for the Policy and Procedures controls identified in NIST SP 800-53. The guide provides SnowBe Online employees, contractors with significant security responsibilities and other IT personnel involved in implementing access control, guidance on the specific procedures they are to follow for implementing AC features and functions for systems under their purview.

AC-02 Account Management

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to SnowBe Online 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.

AC-03 Access Enforcement

The purpose of this document is to define the SnowBe Online policy and procedures for implementing and maintaining appropriate access controls (see Definitions) for State information assets (see Definitions). This document corresponds to the Access Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53.

AC-04 Information Flow Enforcement

This policy is to establish limits on data access and distribution. This policy ensures that information flows within SnowBe Online’s systems are secure, authorized, and compliant with applicable legal and regulatory requirements. By enforcing strict controls over how information is transmitted, accessed, and shared, the policy aims to protect sensitive data, prevent unauthorized access or leakage, and maintain the integrity of business operations.

AC-05 Separation of Duties

This policy is enacted to educate employees on the expectations for dividing key areas of the business. This barrier will reduce the risk of fraud or unauthorized access from other departments.

AC-06 Least Privilege Policy

The purpose of this policy is to establish and enforce the principle of least privilege within SnowBe Online's systems and networks. This policy ensures that users are granted the minimum level of access required to perform their assigned duties, thereby enhancing security.

AC-07 Unsuccessful Logon Attempt Policy

The purpose of this guide is to provide guidance for the Unsuccessful Logon Attempts identified in NIST SP 800-53. This policy provides SnowBe Online employees, contractors with significant security responsibilities and other IT personnel involved in implementing access control, guidance on the specific procedures they are to follow for implementing Unsuccessful Logon Attempts features and functions for systems under their purview.

AC-11 Device Lock

This policy describes the minimum-security policy for mobile devices. Mobile devices must be appropriately secured to

- Prevent sensitive or confidential data from being lost or compromised
- Reduce the risk of spreading viruses
- Mitigate other forms of abuse of the company's computing and information infrastructure

AC-14 Permitted Actions Without Identification or Authentication

This policy outlines the permitted actions that can be taken without requiring identification or authentication, ensuring that SnowBe Online maintains a balance between security and usability. It aims to define the circumstances under which access to certain resources or data can be granted without the need for formal identification or authentication processes.

AC-18 Wireless Access

The purpose of this policy is to state the standards for wireless access to the company's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

AC-19 Access Control for Mobile Devices Policy

This policy establishes the requirements for access control when using mobile devices to access SnowBe's network, systems, and data. It aims to protect company information and customer data by defining rules for mobile device usage and ensuring compliance with security standards.

AC-20 Use of External Systems

The purpose of this policy is to ensure that information shared internally and externally by SnowBe is managed securely. It aims to establish protocols for sharing data to protect customer privacy and prevent unauthorized disclosure of sensitive company information.

AC-21 Information Sharing

The purpose of this policy is to ensure that information shared internally and externally by SnowBe is managed securely. It aims to establish protocols for sharing data to protect customer privacy and prevent unauthorized disclosure of sensitive company information.

AC-25 Reference Monitor

The purpose of this policy is to mediate all access between subjects and objects, enforcing security policies to prevent unauthorized actions such as writing restricted files or reading top secret information.

CM-01 Change Control Management

The purpose of this policy is to ensure that all changes to SnowBe Online IT Resources are tracked, to support continuity of IT services, and reduce negative impact on services and Users.

DEV-01 System Development Life Cycle Policy (SDLC)

The purpose of the Systems Development Life Cycle (SDLC) Policy is to describe the requirements for developing and/or implementing new software and systems at SnowBe Online and to ensure that all development work is compliant as it relates to any and all regulatory, statutory, federal, and /or state guidelines.

DEV-02 Security Maturity Policy

An Enterprise Cybersecurity Maturity Model provides a structure for SnowBe Online to baseline current capabilities in cybersecurity while establishing a foundation for consistent evaluation. By implementing a cybersecurity maturity model, state agencies 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 the agency maturity impacts cybersecurity premiums.

SP-01 PCI DSS 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

SP-02 Password Policy

This policy is to educate SnowBe Online staff on the characteristics of a strong password as well as to provide recommendations on how to securely maintain and manage passwords. The purpose of this policy is to establish a strong password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software

SP-03 Security Awareness Training Policy

The Security Awareness and Training Policy establishes the requirements to assist Information Technology (IT) system managers, administrators, and users of SnowBe Online systems and data the steps to ensure that SnowBe Online systems and data are appropriately safeguarded. Our executives, staff, vice presidents, interns, managers, senior managers, board members, contractors and business partners are the frontline to protecting SnowBe Online's data assets and this policy will assist at providing consistent guidance and overall approach to security awareness

SP-04 Data Retention Policy

This policy is intended to assist SnowBe Online inadequately identifying, protecting, and managing the records it needs to maintain and the process of destroying records that have reached their mandatory retention periods or are no longer necessary for the operations of SnowBe Online. This policy will help ensure that SnowBe complies with all applicable laws and regulations governing records retention and eliminates unnecessary records, which cause storage bloat.

SP-05 Remote Access Policy

The purpose of this policy is to define standards for connecting to SnowBe Online's network from any end user device, for example: PC, Tablet). These standards are designed to minimize the potential security exposure to SnowBe Online from damages which may result from unauthorized use of SnowBe Online resources. Potential damages include the loss of sensitive or SnowBe Online confidential data, intellectual property, damage to public image, and damage to critical SnowBe Online internal systems.

SP-06 Acceptable Usage Policy

The purpose of this policy is to establish what behaviors are acceptable with company devices and on the company network. These guidelines will help to mitigate risk against cyber incidents. This policy will also mitigate risk against behaviors that would cause damage to the company's image.

SP-07 Third Party Vendor Security Policy

The purpose of this policy is to ensure that third-party vendors working with SnowBe Online adhere to our security, data protection, and compliance standards to safeguard customer and company information. This policy outlines the requirements, processes, and responsibilities for the management and oversight of third-party vendor relationships, especially those with access to sensitive data or critical systems. It includes rules to assess, monitor, and manage risks associated with these relationships.

SP-08 Customer Privacy Policy

The purpose of this policy is to establish SnowBe Online's commitment to protecting the privacy of our customers. This document outlines how we collect, use, store, and protect personally identifiable information (PII). Our goal is to be transparent about our data handling practices and to ensure compliance with applicable privacy laws and regulations. By implementing this policy, SnowBe aims to build and maintain the trust of our customers, especially as our business operations rely heavily on online sales and customer interactions.

SP-09 Incident Reporting Policy

Users of SnowBe Online Resources connected to the SnowBe Online network, as well as all users of SnowBe Online Data, must promptly report all actual and suspected Cyber Security Incidents. SnowBe Online IT is responsible for evaluating incidents for a breach of SnowBe Online Data, including Personal Information held by SnowBe Online, and when necessary to initiate the Cyber Security Incident Response Plan. Prompt and consistent reporting of Cyber Security Incidents protects and preserves electronic resources and institutional data and aids SnowBe Online's compliance with applicable law.

SP-10 Computer and Network Security Policy

This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

SP-11 Removable Media Policy

This policy establishes the correct practices with using removable media devices.

SP-12 Patch Policy

This document establishes the Vulnerability and Patch Management Policy for SnowBe Online. This policy defines requirements for the management of information security vulnerabilities and the notification, testing, and installation of security-related patches on devices connected to SnowBe Online networks.

SP-13 Electronic Data Disposal Policy

The purpose of this policy is to provide SnowBe associates guidelines for proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices and electronic media being disposed, recycled or transferred either as surplus property or to another user. The disposal procedures used will depend upon the type and intended disposition of the media. This also is relevant for clients, as a promise of how SnowBe Online will be handling their data.

SP-14 Patch Management Policy

The purpose of this policy is to enforce patch requirements for SnowBe Online-owned or managed IT Resources.

Standards and Procedures

Standards and procedures provide specific, actionable guidelines that support and implement our broader policies, detailing the methods and processes to be followed in order to achieve our security objectives and maintain compliance.

NU-01 New Account Creation Procedure

This procedure outlines the steps for creating user accounts on SnowBe Online Systems. The purpose of this procedure is to detail the steps involved in establishing new user accounts for both internal employees and external customers. It ensures a consistent account creation process throughout the organization.

PP-01 Password Procedure

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of this Procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

PS-01 Password Standard

This standard identifies the minimum password requirements needed to protect SnowBe Online data and systems. Passwords are used on SnowBe Online devices and systems to facilitate authentication, i.e., helping ensure that the person is who they say they are. The security of SnowBe Online data is highly dependent upon the secrecy and characteristics of the password. Compromised passwords can result in loss of data, denial of service for other users, or attacks directed at other Internet users from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of private data such as research participant data, and private employee data.

Section 6: Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will be in place until the policy changes or the person’s employment status changes.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Section 7: Version History Table

Version	Date	Description
1.0	30-Oct-24	Created/Added- Scope, Definitions, Roles & Responsibility, Exceptions/Exemptions, Enforcement
1.1	01-Nov-24	Updated Orphaned Text and Exceptions/Exemptions. Created/Added – Policies Updated Definitions
1.2	02-Nov-24	Updated Policies and Definitions. Fixed Formatting and other issues
2.0	06-Nov-24	Started to update the definitions Adding in the AC and Purpose
2.1	07-Nov-24	Updated additional information for Policies.
2.2	10-Nov-24	Continued to update policies and finalized document
3.0	14-Nov-24	Update with New User procedure and new policy
4.0	18-Nov-24	Getting the document ready for week 4
4.1	20-Nov-24	Updated spacing and terms. Also added a statement section for each document. Added week for standard and procedure.
4.2	21-Nov-24	Adjusted Definitions
4.3	21-Nov-24	Reviewed changed from feedback were done and finalized document.
4.4	24-Mar-25	Added SDLC Policy, Patch Management Policy, and Security Maturity Policy

Citations

Michigan Technological University. (n.d.). *Information Security Plan*. Retrieved from https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://my.wlu.edu/its/about-its/information-security-plan
Definition Roles and Responsibilities

https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-statewide-information-security-program-plan.pdf
Under Organization And Management #6

State of Oregon. (n.d.). *Statewide Information Security Plan*. Retrieved from https://www.oregon.gov/eis/cyber-security-services/documents/statewideinformationsecurityplan.pdf

University at Buffalo. (n.d.). *Incident Response Plan*. Retrieved from https://www.buffalo.edu/ubit/policies/guidance-documents/incident-response-plan.html

Georgia Institute of Technology. (n.d.). *Cyber Security Policy*. Retrieved from https://policylibrary.gatech.edu/information-technology/cyber-security-policy

NIST: National Institute of Standards and Technology. (n.d.). *NIST Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework

TechTarget Definition Glossary Search: TechTarget. (n.d.). *TechTarget IT Glossary*. Retrieved from https://www.techtarget.com/whatis/

PCI Security Standard Glossary: PCI Security Standards Council. (n.d.). *Glossary of Terms*. Retrieved from https://www.pcisecuritystandards.org/pci_security/glossary

Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com

Used to correct grammar errors and spelling errors.

- Systems Development Life Cycle (SDLC) Policy – University of Kansas:

Georgia Technology Authority's Cybersecurity Capability Maturity Model (SS-20-001)