SNOWBE ONLINE
SECURITY PLAN

Christopher Stevens
Date: 10-28-2025
Version 5.0

.

Table of Contents

Section 1: Introduction

The purpose of this plan is to ensure the confidentiality, integrity, and availability of data; define, develop, and document the information policies and procedures that support SnowBe's online goals and objectives; and allow SnowBe Online to satisfy its legal and ethical responsibilities regarding its IT resources.

- Information security policies and procedures represent the foundation for SnowBe Online.
- Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout SnowBe Online.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud, and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business. When consistently applied throughout the SnowBe Online Company, these policies and procedures ensure that information technology resources are protected from a range of threats to ensure business continuity and maximize the return on investments of business interests.

This plan reflects SnowBe Online's commitment to the stewardship of sensitive personal information and critical business information. With acknowledgement of the many threats to information security and the importance of protecting the privacy of SnowBe Online constituents, safeguarding vital business information, and fulfilling legal obligations.

This plan will be reviewed and updated at least once a year. Also, when the environment changes or whichever comes first.

Section 2: Scope

This security plan applies to all SnowBe Online's employees. It encompasses managing and controlling user access privileges to systems, applications, and data resources within our IT infrastructure.

Section 3: Definitions

Access Control
The process of granting or denying specific requests to obtain and use information and related information processing services. Also includes preventing unauthorized access to systems and information.

Access Management
The set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common access management services you encounter every day, perhaps without realizing it, are policy administration, authentication, and authorization.

Authentication Mechanism
Hardware- or software-based mechanisms that force users to prove their identity before accessing data on a device.

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. Risk assessment is 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.

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Data Classification
The process of organizing data into categories based on sensitivity and required security controls (i.e.. Public, internal, confidential, or restricted). This helps ensure appropriate levels for each type of data.

Endpoint
Any device that connects to a network and communicates back and forth with that network. Common examples include laptops, desktops, smartphones, and tablets.

Integrity
Guarding against improper information modification or destruction includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Multi-Factor Authentication (MFA)
An authentication method that requires users to provide two or more verification factors to gain access to a system or resource. This enhances security by requiring a combination of something the user knows (password), has (token or mobile device), or is (biometric).

Principle of least privilege
A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.

Provisioning
The process of setting up a network so that authorized users, devices, and servers can access it. In practice, network provisioning primarily concerns connectivity and security, which means a heavy focus on device and identity management.

Role-based access controls (RBAC)
Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Security Incident
An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information. It also includes interference with system operations in an information system.

Session Timeout
A security feature that automatically logs users out after a period of inactivity. It helps prevent unauthorized access when users leave their devices unattended.

VPN (Virtual Private Network)
A secure connection over the internet that encrypts data between a remote user and the organization's internal network. SnowBe uses VPNs for laptop-based sales access.

Section 4: Roles & Responsibilities

Chief Information Officer (CIO)
Organizing the entire IT infrastructure, from strategy to managing IT systems and driving digital transformation in the business.

- Developing and implementing the organization's IT infrastructure to support business goals.
- Managing the IT staff and overseeing the IT department.
- Implementing processes and developing IT policies.

Chief Information Security Officer (CISO)
In charge of overseeing the businesses' information, cybersecurity, and technology security.

- Developing and implementing information security strategies.
- Enforcing security policies to protect critical data and sensitive IT infrastructure of SnowBe.
- Ensuring SnowBe complies with all relevant industry standards, regulations, and established internal policies.

Cloud Architect
Professional who designs, implements, and manages the company's cloud computing infrastructure.

- Manage, design, and implement SnowBe Online cloud infrastructure.
- Create a cloud strategy aligning with the goals and objectives of SnowBe Online.
- Monitor the performance of the cloud infrastructure and identify potential issues.

Employees
Responsible for following all policies, procedures, and compliances of SnowBe Online while providing exceptional customer service.

- Providing exceptional customer service to all SnowBe customers.
- Adhere to all policies, procedures, and compliances.

Human Resources
In charge of managing the employee lifecycle, including recruitment, termination, and retirement, and ensuring compliance with labor laws.

- Manage recruitment of all new employees and the onboarding process.
- Ensure positive employee relations and compliance.
- Provide training and development of new skills to grow within the company.

IT Staff (Information Technology)
Manage and support SnowBe's technological infrastructure and data.

- Ensuring technology within the business functions smoothly and properly.
- Troubleshoot and manage software and hardware, including operating systems.
- Implement and maintain security measures to protect data from unauthorized access.

Network Architect
In charge of designing, implementing, and managing complex computer networks for SnowBe.

- Design and implement security measures to protect SnowBe's network from vulnerabilities along with any potential threats.
- Monitoring the performance of the network, identifying/resolving problems, and making the necessary adjustments.
- Upgrade and maintain hardware and software, keeping things up to date.

Network Specialist
Ensure that the computer network of SnowBe is functioning securely and efficiently.

- Designing and planning the LAN and WAN networks for SnowBe.
- Documenting network configurations and procedures for SnowBe.
- Troubleshooting network connectivity issues and technical support to end-users.

Security Analyst
In charge of safeguarding SnowBe computer systems and networks from breaches or cyber threats.

- Monitor network traffic and analyze security logs for SnowBe.
- Perform assessments on systems for weaknesses and provide recommended solutions.
- Help in the development of disaster recovery plans for systems and data in case of emergencies.

System Administrators
Will be responsible for the upkeep, configuration, and reliability of SnowBe computer systems and networks.

- Setting up and configuring computer systems, networks, and applications of SnowBe.
- Managing employee accounts of SnowBe, their passwords, and providing necessary technical support.
- Ensuring SnowBe security measures are implemented along with access controls and firewalls.

Third Party Management
Identifying potential risks, they perform diligently in their task to mitigate risks associated with external entities like vendors and suppliers involving performance.

- Evaluating potential third parties before engaging in part of SnowBe Online.
- Making sure contracts clearly define responsibilities, expectations, compliance requirements, and responsibilities for SnowBe Online.
- Perform due diligence and risk assessment on behalf of SnowBe.

Section 5: Statement of Policies, Standards and Procedures

…Security Policies

SDLC 01 - Security Development Life Cycle
This policy ensures that security and data privacy are integrated into every stage of the system lifecycle, from initial concept to retirement.

SM 01 - Security Maturity
This policy outlines the company's commitment to continuously enhancing its security controls, processes, and technologies to protect its assets, customer data, and brand reputation from evolving threats.

PM 01 - Patch Management
This policy aims to protect the company's information systems and data from known exploits by ensuring that software and firmware patches are applied in a timely and systematic manner.

SP 1 - Backup & Disaster Recovery
This policy outlines how SnowBe backs up critical systems and data, and how it will recover from incidents like cyberattacks or hardware failure. It includes backup frequency, storage locations, and testing procedures.

SP 2 - Acceptable Use Policy (AUP)
This policy defines acceptable behavior for using company systems, networks, and data. It prohibits unauthorized access, misuse of resources, and unsafe practices.

SP 3 - Email Security

This policy enforces secure use of email systems, including spam filtering, link scanning, and restrictions on sending sensitive data. It also defines procedures for handling suspicious messages.

SP 4 - Incident Response Plan
This policy defines how SnowBe responds to security incidents, including detection, containment, eradication, and recovery. It also includes roles, communication plans, and post-incident reviews.

SP 5 - Security Awareness & Training
This policy requires all employees to undergo security training during onboarding and annually. It covers phishing, password safety, and reporting suspicious activity.

SP 6 - Remote Access Policy
This policy governs how employees connect to company systems remotely, such as via VPN. It includes multi-factor authentication, session timeouts, and device checks.

SP 7 - Endpoint Security
This policy ensures that all laptops and desktops have antivirus software, firewalls, and the latest security patches. It protects endpoints from malware and unauthorized access.

SP 8 - Network Security
This policy addresses the design, monitoring, and security of SnowBe's internal and external networks. It includes segmentation, VPN enforcement, and secure wireless access.

SP 9 - Password Authentication Policy
This policy enforces the principle of least privilege and defines password complexity, expiration, and storage requirements. It ensures that users only access systems and data necessary for their roles.

SP 10 - Data Retention Policy*)*
This policy defines how long SnowBe retains various types of data and how it is securely disposed of. It ensures compliance with legal and business requirements while minimizing risks.

SP 11 - Data Classification
This policy defines how SnowBe categorizes data (e.g., public, internal, confidential) based on sensitivity and impact. It ensures appropriate handling, storage, and access controls for customer and business data.

SP 12 - Firewall Policy
This policy governs the configuration and maintenance of firewalls protecting SnowBe's network. It includes rules for blocking unauthorized access and periodic reviews of rules.

SP 13 - 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 the unit and the SnowBe Online company.

…Access Control Policies

AC 1 - Policy and Procedure
The purpose of this policy is to establish, document, and maintain access control policies and procedures that govern the management of user and system access to SnowBe Online's information systems. Given the

company’s rapid growth and previously informal approach to IT management, a formalized policy is essential to support consistent and secure access practices. This policy ensures alignment with NIST 800-53 standards and supports regulatory compliance, especially as SnowBe prepares to go public.

AC 2 - Account Management
The purpose of this policy is to define how user accounts are created, managed, and deactivated. With employees having broad and often unnecessary access to sensitive systems, strict account management is vital to limit risk and enforce accountability. This policy supports role-based access control and ensures timely removal of access when users change roles or leave the organization.

AC 3 - Access Enforcement
This policy ensures that system-enforced controls restrict access to authorized users and activities based on established rules. Access enforcement mechanisms are necessary for SnowBe Online to prevent unauthorized users from accessing sensitive financial and customer data, especially on their AWS-hosted platform and internal servers. The policy also aligns with PCI compliance requirements, which mandate strict control over who can access payment-related information.

AC 4 - Information Flow Enforcement
This policy governs how data is permitted to flow between different systems and components within the SnowBe network. Given the blend of AWS cloud systems, on-premises servers, and remote devices, controlling the flow of sensitive data is crucial. It helps prevent data leakage, supports regulatory compliance, and protects against unintentional exposure of customers and financial information.

AC 5 - Separation of Duties
The purpose of this policy is to reduce the risk of fraud or error by dividing responsibilities among multiple individuals. SnowBe Online must ensure that no single individual has full control over critical operations like system configuration, transaction processing, and approval workflows. This separation supports internal controls and enhances accountability across departments.

AC 6 - Least Privilege
This policy ensures that users are granted only the access rights they need to perform their job functions. SnowBe Online's current practice of allowing employees access to all servers poses a significant risk. Implementing least privilege mitigates the risk of insider threats and accidental data breaches by limiting unnecessary access.

AC 7 - Unsuccessful Login Attempts Policy
The purpose of this policy is to lock user accounts or initiate alerts after a defined number of failed login attempts. This helps to prevent brute-force attacks and unauthorized access to SnowBe Online’s systems. By locking out accounts temporarily, the policy provides a protective mechanism for both on-premises and cloud-hosted systems.

AC 8 - System Use Notification
This policy ensures that users are presented with a login banner that informs them of authorized use expectations. It helps SnowBe Online reinforce awareness that systems are monitored, and usage is subject to policy enforcement. The banner acts as a legal deterrent against misuse and supports forensic investigations if needed.

AC 9 - Previous Login Notification

This policy notifies users of their last login attempt and alerts them to any unauthorized access. By implementing this feature, SnowBe Online adds a layer of user-driven accountability and anomaly detection. It empowers users to identify suspicious activity tied to their accounts.

AC 11 - Device Lock
This policy requires automatic locking of devices after a period of inactivity to prevent unauthorized access. With 50 company endpoints including laptops used in the field, enforcing device lock is critical. This reduces the risk of sensitive data exposure due to unattended systems in retail or public environments.

AC 12 - Session Termination
This policy mandates automatic termination of user sessions after a designated period of time. It ensures that active sessions don't remain open, especially in shared workspaces or over remote VPN connections. This measure supports secure operation and is vital in protecting customer data accessed via remote laptops.

AC-16 - Security and Privacy Attributes
Implementing metadata tags on sensitive information enables policy enforcement and automation. This control supports future maturity in access control enforcement.

AC 17 - Remote Access Control
This policy governs how users connect to company systems from outside the internal network. SnowBe Online uses VPNs to allow sales staff to access applications remotely, so controls must ensure secure authentication, encryption, and activity monitoring. The policy ensures that only approved remote devices and users can access company data.

AC 18 - Wireless Access
The purpose of this policy is to secure wireless network access within SnowBe's facilities. As retail locations and the LA office use wireless connections, protections must be in place to prevent unauthorized use and intercepts. This policy ensures encryption standards are followed, and only company-approved devices can connect.

AC 19 - Access Control for Mobile Devices
This policy regulates the use of mobile devices (e.g., smartphones, tablets) that access company resources. With growing mobility, SnowBe Online must assess, authorize, and manage mobile devices to prevent data loss or compromise. The policy supports secure mobile use and aligns with best practices for data protection.

AC 21 - Information Sharing
This policy controls how information is shared internally and externally, ensuring it's only shared with authorized parties. SnowBe Online must protect sensitive customer and vendor information shared between departments and with third-party partners. The policy helps preserve confidentiality and integrity in business operations and communications.

…Cryptography and Encryption Control Policies

AC-23 - Data Mining Protection
To prevent unauthorized pattern analysis of stored customer data, this control limits data aggregation and correlation. This is more of a future consideration as SnowBe grows.

CP-9 - System Backup
The company must ensure regular backup procedures are in place and effective to recover data loss or ransomware. With critical business data hosted on both AWS and on-prem servers, this control supports operational resilience, recovery, and business continuity.

IA-2 – Identification and Authentication (Organizational Users)
SnowBe employees currently have access to nearly all data, which makes user identification and authentication a top priority. This control ensures only authorized users access sensitive systems and data. SnowBe must ensure that only authorized users can access systems and data, especially given the unrestricted access currently in place. This control establishes identity verification as the foundation of access security.

IA-5 – Authenticator Management
Without effective password and token management, compromised credentials could give attackers full access to systems. To secure access, SnowBe must implement proper password policies and management practices. Without this, compromised credentials could lead to unauthorized access to the system. This control enforces strong password policies and secure authenticator lifecycle management.

IA-7 – Cryptographic Module Authentication
SnowBe must ensure that cryptographic mechanisms used in the environment (e.g., for VPN, HTTPS, and encrypted data) are authenticated and validated. This control guarantees the use of trusted modules.

MP-6 – Media Sanitization
Before repurposing or disposing of storage media, it must be sanitized to remove residual data. This is essential for protecting stored customer and payment data. Before any storage media is reused or discarded, it must be wiped or destroyed securely. This ensures customer and payment data aren't recoverable.

MP-5 – Media Transport
Sensitive media transported between offices or off-site must be protected during transit. This control enforces secure handling and logging of physical media.

SC-4 – Information in Shared System Resources
With multiple users accessing shared servers, it's critical to ensure information is not unintentionally leaked or accessed via shared resources like RAM or cache. This control helps reduce covert channel risks.

SC-7 – Boundary Protection
SnowBe's hybrid infrastructure must protect the boundary between internal and external networks. Requiring strong boundary defenses to prevent unauthorized access and to reduce exposure to threats. Firewalls, intrusion detection, and segmentation are essential to control traffic flows.

SC-8 – Transmission Confidentiality and Integrity
SnowBe's customer data needs to be protected from interception or tampering. The use of VPNs and online transactions requires secure communication channels. This control enforces encryption and integrity checks for transmitted information.

SC-12 – Cryptographic Key Establishment and Management
SnowBe needs proper key management to support secure communications and storage encryption. Strong encryption depends on well-managed keys. This control ensures that the generation, distribution, revocation, and destruction of keys are done securely to support its encryption strategy.

SC-13 – Cryptographic Protection
General cryptographic protections are needed for both data in transit and at rest. Given the sensitive data handled, cryptographic methods must be applied broadly for confidentiality and integrity. SnowBe relies heavily on web-based systems and must ensure encryption is applied throughout. This control enables protection beyond simple access mechanisms.

SC-17 – Public Key Infrastructure Certificates
SnowBe needs a trustworthy PKI to manage digital certificates for secure communication. This is a foundation for authentication, email security, and encrypted web sessions.

SC-20 – Secure Name/Address Resolution Service (Authoritative Source)
To defend against DNS spoofing or redirection attacks. SnowBe needs secure DNS practices and must secure its DNS lookups. This is especially important for online sales and cloud services on AWS. This control protects against impersonation attacks on their public websites.

SC-28 – Protection of Information at Rest
Since credit cards and customer data are stored indefinitely on the website database, encryption at rest is essential and very critical. This control ensures that even if the system or storage is compromised, the data remains secure.

SC-37 – Out-of-Band Channels
In case primary systems are compromised, SnowBe should consider out-of-band communication for alerts or control. This is important for maintaining operations during incident response.

SI-7 – Software, Firmware, and Information Integrity
The consultant highlighted a need for patching, antivirus updates, and outdated firmware, making system integrity controls critical. This control detects and prevents unauthorized changes such as malware or tampering. Ensures system integrity to software and configurations.

SR-12 – Component Disposal
SnowBe should implement secure disposal procedures for old devices storing sensitive data. Improper disposal of retired laptops, servers, or storage could lead to data breaches. This control prevents data leakage, mandates secure sanitization, and destruction of components to avoid improperly discarded hardware.

…Standards and Procedures

CCM-1 - Change Control Management
The purpose of this Change Control Management Policy is to establish a structured process for managing changes to SnowBe Online's IT systems, applications, and infrastructure to ensure stability, security, and compliance. It aims to minimize risks, prevent unauthorized changes, and maintain the integrity of the AWS hosted e-commerce platform, customer data, and PCI compliance requirements. This policy outlines procedures for proposing, reviewing, approving, implementing, and documenting changes to safeguard operations and customer trust.

NAC-1 - New Account Creation Procedure
The purpose of this New Account Procedure is to establish a standardized process for creating and managing user accounts for SnowBe Online's IT systems, ensuring secure access to the AWS platform, servers, and customer data. It aims to enhance security, comply with PCI standards, and address past access management deficiencies by defining clear steps for account creation, verification, and approval.

PSWS-1 - Password Standards
The purpose of SnowBe Online's Password Standard is to establish clear and consistent guidelines for the creation, management, and protection of all passwords used to access SnowBe Online's IT systems and data. This standard exists to fortify our overall security posture by mitigating risks associated with weak, compromised, or misused credentials. It aims to prevent unauthorized access to sensitive information, including customer data and financial details, thereby ensuring compliance with critical regulatory requirements such as PCI DSS. This standard outlines the specific requirements for password complexity, length, uniqueness, and expiration, applying to all employees, contractors, and third-party vendors. It also details the procedures for

password changes, resets, and the secure handling of credentials. By defining these robust parameters, SnowBe Online strives to enhance the integrity, confidentiality, and availability of its IT resources and safeguard against cyber threats.

PSWP-1 - Password Procedure
The purpose of SnowBe Online's Password Procedure is to provide clear, step-by-step instructions for all users on how to effectively manage their passwords in accordance with the SnowBe Online Password Standard. This procedure exists to ensure that all individuals interacting with SnowBe Online's IT systems understand and can consistently apply the security measures necessary to protect their credentials and, by extension, sensitive company and customer data. It outlines the specific actions required for creating strong passwords, securely changing passwords, resetting forgotten passwords, and reporting any suspected password compromises. By adhering to this procedure, SnowBe Online aims to minimize the risk of unauthorized access, enhance overall system security, and maintain compliance with data protection regulations.

Section 6: Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not

constitute a permanent change to the policy.

Section 7: Version History Table

Version	Date	Description
1.0	5-8-2025	Added Cover Page, Purpose Scope, Role and Responsibilities, Exceptions/Exemptions, Enforcement, Citations
1.1	5-12-2025	Correction made to Scope Statement, Font, Paragraph spacing, Member Section numbers, added Citations,
2.0	5-19-2025	Policy number corrections, PCI Policy added, Format corrections, Access Controls added
3.0	5-26-2025	Update Security Plan with Cryptography and Encryption Controls
4.0	6-1-2025	Update Security Plan with Standards and Procedures
5.0	10-28-2025	Update Security Plan with three new Security Policies

Citations

Policy Template
https://www.sans.org/information-security-policy/
Introduction, Scope, Roles and Responsibilities, Exceptions/Exemptions

Michigan Technical Institute
https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf
Introduction, Scope,

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, Statements of Policies, Standards and Procedures, but as a group we revised the verbiage.

Roles & Responsibilities
https://security.berkeley.edu/roles-and-responsibilities-policy
https://www.thebalancemoney.com/corporate-job-titles-2061491

Written by Jordan Valdez (General terms searched through Google)

Fordham University (Change Control)
https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/change-control-policy/
Purpose, Scope, Definitions

Montclair State University (Account Creation)
https://www.montclair.edu/policies/all-policies/account-management-policy/
Purpose, Scope (Reworded from a couple google searches)

Haverford College (Account-Creation-and-Deletion-Policy)
https://www.haverford.edu/sites/default/files/Office/IITS/Account-Creation-and-Deletion-Policy.pdf
Cited mostly as a reference to verbiage used to rewrite the purpose, scope, and procedures.

Rock Vally College
https://rockvalleycollege.edu/_resources/files/procedures/2-30-060-Procedure-Passwords.pdf
Purpose Scope Procedure