SNOWBE ONLINE SECURITY PLAN

Group Member Names:
Emmanuel Estrella
Jediah Louis
Matias Cabrera Peralta
Nolan Fraser
Rayanthony Ramos

Version #2.0
Date: 11/24/2025

Table of Contents

Section 1: Introduction

The Information Security Plan establishes and states the policies governing SnowBe Online IT standards and practices. These policies define the Company's objectives for managing operations and controlling activities. These policies represent the plans or protocols for achieving and maintaining internal control over information systems as well as compliance with the requirements imposed on the company.

Section 2: Scope

This security plan covers every electronic system SnowBe uses to run its business. It includes the main website and online store, which are hosted on AWS, as well as all customer data and credit card information the company currently stores. It also applies to all devices used in our offices and retail locations in the U.S. and Europe. This includes office desktop computers, the laptops used by the sales team when they connect through the VPN, and all of our critical servers used for order management, customer information, accounting, and internal applications. The purpose of this plan is to fix the major security problems that were identified, such as outdated software, overly broad employee access, and servers that are not physically secured. It also ensures that credit card data is properly protected so SnowBe can meet PCI requirements and operate as a secure, professional, and publicly traded company.
This security plan applies to every employee, contractor, third-party vendor and every electronic system SnowBe uses to run its business. It covers the main website and online store hosted on AWS, all customer data and credit card information we store, and all devices used in our offices and retail locations in the U.S. and Europe. This includes office desktop computers, the laptops used by sales and remote staff when they connect through the VPN, and all critical servers used for order management, customer information, accounting, and internal applications. All employees are expected to follow this security plan whenever they access, handle, or manage SnowBe systems and data.

Section 3: Definitions

ACLs (Access Control Lists)
Lists that define which users or systems are allowed to access certain data or resources.
eing responsible for actions, decisions, or outcomes.

Adhering
Following rules, laws, or standards closely.

API (Application Programming Interface)
A tool that allows different software programs to communicate and work together.

AWS (Amazon Web Services)
A large cloud service SnowBe uses to host its website and store customer information.

CDE (Cardholder Data Environment)
All systems and networks that store, process, or transmit credit card information.

CEO (Chief Executive Officer)
The highest-ranking person who oversees the entire company.

CFO (Chief Financial Officer)
The leader responsible for managing the company's money and financial decisions.

CIO (Chief Information Officer)
The executive responsible for all technology systems and data security at SnowBe.

Cloud Storage Facility
An online service used to store files and data safely on the internet.

COO (Chief Operating Officer)
The executive who manages day-to-day business operations.

Compensating Controls
Alternative safety measures used when the normal required control cannot be put in place.

Configuration
How a system, device, or program is set up.

Credential-Based Attacks
Cyberattacks where criminals try to steal or guess usernames and passwords.

Framework
A structured set of rules or guidelines.

Granular Access Management
Very detailed control over who can access what parts of a system.

Hardening
Making systems more secure by removing weaknesses.

Mechanisms
Tools or methods used to make something work.

PCI DSS (Payment Card Industry Data Security Standard)
Security rules that companies must follow when handling credit card data.

Privileged Access
Special permissions that allow users to change important settings or data.

Publicly Traded Company
A company that sells its shares on the stock market.

Recovers / Recovery
Returning systems to normal after a problem or attack.

Structured
Organized in a clear and logical way.

Users
People who access and use systems, data, or devices.

VPN (Virtual Private Network)
A secure connection employees use to access SnowBe's systems from outside the office.

Vulnerabilities
Weaknesses in systems that attackers could exploit.

Section 4: Roles & Responsibilities

The security and protection of SnowBe's IT resources are a shared responsibility, mandated by the Executive Management Team and enforced throughout the organization, focused on implementing the necessary NIST 800-53 controls and achieving PCI compliance.

Executive Management & Owners

- **SnowBe Owners/Management Team:**
  - Holds ultimate accountability for funding the security overhaul required to take the company public.
  - Must formally approve the budget necessary to address all consultant-identified fixes (e.g., software licensing, staff training).
  - Required to officially endorse and enforce new security policies to replace the previously "laid-back culture."
- **Chief Information Officer (CIO):**
  - Serves as the single point of contact responsible for the overall security posture and logical position of SnowBe's core infrastructure.
  - Must be formally notified of any significant security changes made by other entities connected to SnowBe's network (as defined in the Scope).

Technical Operations & Maintenance

- **E-commerce & AWS Team:**
  - Responsible for the security, patching, and hardening of the AWS platform hosting the website and online store.
  - Must immediately update the company's WordPress shopping cart.
  - Holds primary responsibility for the security of the website database where credit card and customer history are stored, driving immediate PCI compliance efforts.
- **Server & Network Administration:**
  - Responsible for physical security by locking the servers in a secured area of the office.
  - Must immediately update the firmware of all network devices.
  - Responsible for applying patches for all Windows servers.
  - Must correct the broad access issue by implementing granular Access Management

controls on all servers (on-premise and AWS).

- **Endpoint & Systems Management Team:**
  - Responsible for applying patches for all PCs and laptops (desktops/laptops in LA office and remote sales laptops).
  - Must update the Anti-Virus and backup software across all endpoints.

Users & Enforcement

- **Technical Consultant:**
  - Provides initial oversight and strategic direction for implementing the NIST 800-53 framework.
  - Responsible for guiding internal teams through the urgent steps needed to achieve system control and PCI compliance.
- **All Employees (Sales, Accounting, Customer Support):**
  - Must adhere to all new security policies, especially those related to restricted Access Management on servers and systems.
  - Must ensure the security of the devices they use for work (e.g., Laptops using the VPN connection).
  - Responsible for immediately reporting any security incidents or suspicious physical activity.

Section 5: Statement of Policies, Standards and Procedures

Policies

(AC-1) Policy and Procedures
Establishes the governance foundation for the Access Control family. It requires SnowBe to document and disseminate a Policy defining access rules and Procedures for implementation. Periodic reviews, typically annual, are mandatory. This control ensures that all subsequent technical controls (AC-2 through AC-25) are properly managed, authorized, and compliant.

(AC-2) Account Management
governs the full lifecycle of system accounts. It requires SnowBe to control the creation, modification, and termination of user identifiers. Key mandates include verifying authorization before account creation, conducting periodic reviews, and automatically disabling inactive or terminated accounts. This ensures that only authorized users maintain access to organizational information systems.

(AC-3) Access Enforcement
A security control that makes sure systems actually enforce the access rules (who can do what) defined in your policies and ACLs, so users can only access data and functions they're explicitly authorized to use.
(AC-4) Information Flow Enforcement
Information Flow Enforcement requires control and restricts how information flows within and between systems to ensure data only moves through approved, secure, and authorized channels. It prevents unauthorized transfers by enforcing policies using mechanisms like firewalls, filters, segmentation, and data-validation controls.

(AC-5) Separation of Duties
Separation of Duties requires SnowBe to divide critical tasks among multiple individuals so no single person can perform high-risk actions alone. This control prevents fraud, abuse, unauthorized system changes, and misuse of privileged access. By assigning different responsibilities across roles such as Accounting, IT, and Sales, SnowBe reduces insider threats and strengthens overall operational integrity.

(AC-6) Least Privilege
Least Privilege requires SnowBe to restrict each user's access rights to only the minimum necessary to perform their job duties. This applies to system accounts, administrative privileges, processes, APIs, and automated tasks. Enforcing least privilege minimizes the potential impact of account compromise, prevents unauthorized access to sensitive information, and supports PCI DSS and NIST compliance requirements.

(AC-7) Unsuccessful Logon Attempts
Unsuccessful Logon Attempts requires to limit the number of consecutive failed logon attempts and take appropriate actions, such as temporarily locking accounts, delaying further attempts, or notifying administrators, to protect systems from brute-force attacks and unauthorized access. It also supports alternative authentication methods and mobile device protections to maintain security while ensuring availability.

(AC-11) Device Lock
AC-11 Device Lock ensures that SnowBe's systems automatically lock after a period of inactivity to prevent unauthorized access when a user steps away from a workstation, laptop, or mobile device. This control protects sensitive customer and payment data from being exposed through unattended devices in offices, storefronts, or remote environments. Device Lock is essential for preventing misuse, shoulder surfing, or unauthorized physical access, especially given SnowBe's laptops used in sales and support operations.

(AC-12) Session Termination
AC-12 Session Termination requires SnowBe's systems to automatically terminate user sessions after predefined conditions, such as inactivity, completion of a transaction, or security timeouts. This prevents unauthorized individuals from hijacking open sessions or lingering authenticated connections. By enforcing strict session limits across web applications, VPNs, and internal systems, SnowBe reduces the risk of account compromise, protects its AWS-based e-commerce application, and supports PCI DSS requirements for secure session management.

(AC-17) Remote Access
Remote Access is to ensure secure, authorized, and monitored connections to SnowBe Online systems when users access company resources from outside corporate locations. Given SnowBe's use of VPN access for sales laptops, AWS administration, and remote employees, strong remote access controls are required.

(AC-18) Wireless Access
Wireless Access ensures that SnowBe authorizes, secures, and controls all wireless technologies used across stores, offices, and remote environments. It requires strong encryption (e.g., WPA3),

authentication, monitoring for rogue access points, and prohibiting unauthorized wireless devices. This control protects cardholder data, prevents network intrusion via Wi-Fi, and supports segmentation required by PCI DSS for retail and e-commerce environments.

(AC-19) Access Control for Mobile Devices
Access Control for Mobile Devices requires SnowBe to manage, secure, and monitor mobile systems such as laptops, tablets, and smartphones that access company resources. It includes enforcing encryption, authentication, remote wipe, device configuration standards, and restrictions on storing sensitive data. This control protects SnowBe from data loss, mobile malware, unauthorized access, and risks associated with remote or traveling employees.

(SP-1) PCI DSS Policy
This policy applies to anyone involved in handling payment card information for SnowBe, including employees, contractors, third-party vendors, partners, and any systems or networks that process card data. It also covers any SnowBe unit or service that uses third-party software to process transactions. This includes all forms of cardholder data—whether it is being transmitted, stored, or processed—and applies to both electronic and paper formats.

(SP-2) Risk Management Policy
This section details the mandatory requirements for utilizing the NIST Risk Management Framework (RMF) and integrating PCI DSS risk requirements to manage SnowBe Online's information security risks.

(SP-3) Physical Security Policy
This section details the mandatory physical security controls for SnowBe Online's facilities and assets, directly addressing the requirements of the NIST SP 800-53 Revision 5 PE (Physical and Environmental Protection) control family and PCI DSS v4.0 Requirement 9 (Restrict Physical Access to Cardholder Data).

(SP-4) Password Policy
Defines SnowBe’s standards for creating, managing, and protecting passwords to prevent unauthorized access to company systems and data. Requires strong authentication practices, regular password updates, and safeguards to reduce credential-based attacks.

(SP-5) Endpoint Security Policy
Establishes security requirements for all SnowBe laptops, desktops, mobile devices, and other endpoints that access company resources. Ensures devices are properly configured, monitored, and protected against malware, unauthorized access, and data loss.

(SP-06) Email Security Policy
Provides rules for secure use of SnowBe’s email systems to prevent phishing, malware infections, and data leakage. Defines acceptable use, scanning requirements, and user responsibilities for maintaining safe communication practices.

(SP-7) Vulnerability Management Policy
Defines SnowBe’s process for identifying, assessing, prioritizing, and remediating vulnerabilities across systems, applications, and infrastructure. Ensures timely patching and risk-based mitigation to

reduce exposure to exploitation.

(SP-8) Patch Management Policy
Establishes a structured approach for evaluating, testing, approving, and deploying patches to SnowBe systems. Ensures critical updates are applied within defined timelines to protect against known vulnerabilities and maintain system integrity.

(SP-9) Data Retention and Deletion Policy
Specifies how long SnowBe must retain different categories of data based on legal, regulatory, and business requirements. Defines secure deletion processes to ensure outdated or unnecessary data is removed to reduce privacy and security risks.

(SP-10) Security Awareness and Training Policy
Ensures all SnowBe employees and contractors receive ongoing cybersecurity training to recognize threats and follow safe practices. Establishes mandatory education programs to build a strong security culture and reduce human-related risks.

(SP-11) Incident Response Policy
Defines SnowBe's structured process for detecting, reporting, analyzing, containing, and recovering from security incidents. Ensures rapid response and clear communication to minimize damage, restore operations, and meet regulatory requirements.

Standards and Procedures

Section 6: Exceptions/Exemptions

Exceptions or formal exemptions to the requirements defined within this IT Security Plan must be approved through a formal, tiered process reflecting the company's new status as a publicly traded entity requiring strict PCI DSS and NIST 800-53 adherence.

- **Approval Authority:**
  - All minor exceptions must be formally documented and approved by the Chief Information Security Officer (CISO) or the Head of IT who manages the security program.
  - Any exception that significantly increases the risk to the Cardholder Data Environment (CDE) or severely compromises a mandated NIST 800-53 control must also receive final approval from a member of the Executive Management Team (CEO, COO, or CFO).
- **Documentation and Review:**
  - All exceptions will be formally documented, including the business justification, compensating controls (alternative protections) in place, and the duration of the exemption.
  - All plan exceptions will be reviewed on a periodic basis (no less than annually) or whenever the system configuration or underlying business justification changes, to ensure continued appropriateness.

Section 7: Version History Table

Version	Date	Description
1.0	11/24/2025	First Draft
1.1	12/6/2025	Added Access Control Policies,
2.0	12/8/2025	Added Statement of Policies, Standards and Procedures Updated Roles and Responsibilities

Citations

The University of Tennessee, Knoxville. (2015). *Information security program plan*. Office of Information Technology. https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf

Howard University. (2020). *Information security plan*. Enterprise Technology Services. https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf

Oregon Enterprise Information Services, Cyber Security Services. (n.d.). *Statewide information security plan*. Retrieved November 24, 2025, from https://www.oregon.gov/eis/cyber-security-services/documents/statewideinformationsecurityplan.pdf

Johnson & Wales University. (n.d.). *Written information security plan (WISP)*. Information Technology Security Services. Retrieved November 24, 2025, from https://sites.jwu.edu/itss/pdfs/writteninformationsecurityplan.pdf

Virginia Information Technologies Agency. (2022). *2022 Virginia Cybersecurity Plan*. Commonwealth Security. https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/meetings/2022-Virginia-Cybersecurity-Plan.pdf

Google. (2025). *Gemini* (Flash 2.5) [Large language model]. Retrieved November 24, 2025, from https://gemini.google.com/

(used in Exceptions/Exemptions, Enforcement, Roles & Responsibilities, Definitions, Introduction)

OpenAI. (2025). ChatGPT (February 2025 version) [Large language model]. https://chat.openai.com/

(used in Exceptions/Exemptions, Enforcement, Scope, Definitions)