SNOWBE ONLINE SECURITY PLAN

Douglas, Malik
Montgomery, Elijah
Prescod, Ariel

April 28th, 2025

Table of Contents

Purpose

The purpose of this security plan is to assist SnowBe Online in strengthening its information security posture during its transition from a startup to a publicly traded company. As the majority of transactions are processed through its website and customer data is retained indefinitely, implementing formal security policies is critical.

This plan is structured around the ISO/IEC 27001 standard, an internationally accepted framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Adoption of this standard offers a systematic, risk-based approach to protecting sensitive information while ensuring confidentiality, integrity, and availability (International Organization for Standardization [ISO], 2022).

In addition to improving risk posture, ISO/IEC 27001 enhances operational efficiency, incident preparedness, and compliance with industry regulations. As SnowBe Online grows, adherence to these international standards will improve customer trust and organizational accountability.

Scope

This plan applies to all SnowBe Online systems, personnel, and physical locations. It includes hardware such as desktops, laptops, servers, and cloud infrastructure, including services provided by Amazon Web Services (AWS). The plan applies to all employees retail, sales, support, and administrative as well as third-party consultants who access or manage company systems. Any individual or system interacting with company data, payment information, or system configurations is included in this scope.

Definitions

Access Control (AC) – Security techniques and mechanisms that manage who can view or use resources in a computing environment.

Authenticator Management (IA-5) – The control of processes for issuing, managing, and revoking authentication credentials like passwords and tokens.

Boundary Protection (SC-7) – Measures taken to monitor and control communications at the external boundary of an information system to prevent unauthorized access.

Component Disposal (SR-12) – Secure removal and destruction of hardware and components to prevent data leaks.

Cryptographic Key Management (SC-12) – The process of handling cryptographic keys, including their generation, storage, protection, and destruction, to ensure secure encryption practices.

Data Mining Protection (AC-23) – Techniques to prevent unauthorized analysis and extraction of valuable patterns from large data sets.

General Data Protection Regulation (GDPR) – Governs how organizations collect, process, store, and protect personal data.

Health Insurance Portability and Accountability Act (HIPAA) – U.S. federal law passed in 1996 that sets standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

Incident Response (IR) – A systematic approach to addressing and managing the aftermath of a security breach or cyberattack.

Information Security Management System (ISMS) – A structured set of policies and procedures aligned with ISO/IEC 27001, designed to manage and protect sensitive data systematically across an organization.

Information Technology (IT) – The use of computer systems, networks, and software to store, retrieve, transmit, and manage data.

International Organization for Standardization (ISO) – An international body that develops and publishes global standards, including those for information security management, such as ISO/IEC 27001.

Media Sanitization (MP-6) – Processes used to securely erase data from storage devices to ensure data cannot be recovered by unauthorized individuals.

Multi-Factor Authentication (MFA) – A security system that requires multiple forms of verification—such as a password and a code sent to a mobile device—to grant access to systems and applications.

Out-of-Band Communication (SC-37) – Using a separate communication path (different from the primary network) to transmit sensitive information securely.

Payment Card Industry Data Security Standard (PCI DSS) – A set of global standards aimed at securing credit card transactions and protecting cardholder information, required for any organization that handles credit card data.

Public Key Infrastructure (PKI) – A framework for managing digital certificates and public-key encryption to secure communications.

Remote Access (AC-17) – The ability for authorized users to access systems or networks from a location outside the organization’s physical premises.

Secure Name/Address Resolution Service (SC-20) – Security mechanisms applied to DNS and similar services to prevent attacks like DNS spoofing.

Security Attributes (AC-16) – Properties associated with information systems or data that determine security handling requirements, such as sensitivity or confidentiality level.

Software, Firmware, and Information Integrity (SI-7) – Measures that ensure software, firmware, and information are free from unauthorized modification.

Structured Query Language (SQL) – A standard programming language used to manage and manipulate relational databases, often used for querying and updating data in web applications.

System Backup (CP-9) – The process of creating and storing copies of data or system configurations to allow recovery in case of loss or corruption.

Transmission Confidentiality (SC-8) – The protection of information while it is transmitted over a network to prevent interception and unauthorized disclosure.

Uniform Resource Locator (URL) – The address used to access websites and other resources on the internet, usually including the protocol (e.g., HTTPS), domain name, and path.

Virtual Private Network (VPN) – A secure, encrypted connection over the internet that allows users to access internal systems or data as if they were on a private network, improving privacy and data protection.

Roles & Responsibilities

Chief Executive Officer (CEO) - Oversees the security strategy and ensures resources are allocated.

IT Director - Manages security tools, oversees compliance, and coordinates with the technical consultant.

System Administrator - Implements and maintains server, software, and access control security.

Retail Staff - Operate store systems responsibly and report security issues.

Sales Team (Laptop Users) - Use VPN and follow mobile security rules.

Customer Support - Ensure desktops are used securely and follow data protection guidelines.

Statement of Policies, Standards and Procedures

Policies

Access Control Policy (AC-1)

This policy sets the rules for granting, reviewing, and revoking user access to systems, data, and applications based on job roles and the principle of least privilege. It is critical to preventing unauthorized access and ensuring that employees can only access information necessary for their duties. It also includes provisions for account reviews and auditing access logs.

Data Retention Policy (DR-1)

This policy governs how long different types of data are stored before being securely deleted or archived. It ensures compliance with legal and regulatory obligations while also helping manage storage costs and reduce liability. The policy defines data types, retention periods, and secure disposal methods.

Encryption Policy (EP-1)

The Encryption Policy ensures that sensitive data—whether at rest or in transit—is adequately protected using strong encryption techniques. This policy is vital for maintaining data confidentiality, preventing unauthorized access, and meeting regulatory requirements such as HIPAA, GDPR, or PCI-DSS. It also defines acceptable encryption standards and key management practices.

Firewall Policy (FP-1)

The Firewall Policy establishes guidelines for the configuration and management of firewall devices to protect the organization's network perimeter. It ensures only authorized traffic is allowed in and out of the network, reducing the risk of unauthorized access, data breaches, or malicious attacks. The policy also defines rules for firewall rule changes and periodic reviews.

Incident Response Policy (IR-1)

This policy outlines the structured approach an organization must take when a cybersecurity incident occurs. Its purpose is to ensure that incidents are identified, contained, investigated, and resolved efficiently to minimize damage and recover quickly. It also defines roles and responsibilities, communication protocols, and documentation requirements to support compliance and continuous improvement.

Password Management Policy (PM-1)

The Password Management Policy defines the requirements for creating, storing, and changing passwords across systems. It promotes the use of strong, unique passwords and may include guidelines for multi-factor authentication, password expiration, and prohibited password patterns. Its goal is to reduce the likelihood of compromised accounts.

PCI DSS Compliance Policy (PCI-1)

The PCI DSS Compliance Policy establishes requirements for protecting payment card information processed, stored, or transmitted by SnowBe Online. This policy ensures that the organization meets the Payment Card Industry Data Security Standard (PCI DSS) requirements to maintain customer trust and avoid penalties. It

includes guidelines for secure payment processing, restricted access to cardholder data, encryption of payment information during storage and transmission, regular vulnerability scanning, and maintaining a secure network environment. Employees handling card data must follow all PCI DSS procedures, and third-party service providers must demonstrate PCI DSS compliance before engagement.

Individually Selected Access Controls

Ariel Prescod

AC-5 Separation of Duties & AC-6 Least Privilege

AC-6(5) Privileged Accounts
AC-6(9) Log Use of Privileged Functions

AC-18 Wireless Access

AC-18(1) Authentication and Encryption
AC-18(4) Restrict Configurations by Users

Elijah Montgomery

AC-17 Remote Access

AC-17(1) Monitoring and Control
AC-17(2) Protection of Confidentiality

AC-21 Information Sharing

AC-21(1) Automated Decision Support
AC-21(2) Information Search and Retrieval

Malik Douglas

AC-2 Account Management

AC-2(3) Disable Accounts
AC-2(5) Inactivity Logout

AC-7 Unsuccessful Login Attempts

AC-7(2) Purge or Wipe of Mobile Device
AC-7(3) Biometric Attempt Limiting

Individually Selected Controls

Ariel Prescod

AC-17 Remote Access

- Monitoring and Control
- Protection of Confidentiality and Integrity Using Encryption
- Managed Access Control Points
- Privileged Commands and Access

- Protection of Mechanism Information
- Additional Protection for Security Function Access
- Disable Nonsecure Network Protocols
- Disconnect or Disable Access
- Authenticate Remote Commands

SC-7 Boundary Protection

- Physical Separated Subnetworks
- Public Access
- Access Points
- External Telecommunications Services
- Deny by Default – Allow by Exception
- Response to Recognized Failures
- Split Tunneling for Remote Devices
- Route Traffic to Authenticated Proxy Servers
- Restrict Threatening Outgoing Communications Traffic
- Prevent Exfiltration
- Restrict Incoming Communications Traffic
- Host-Based Protection
- Isolation of Security Tools, Mechanisms, and Support Components
- Protect Against Unauthorized Physical Connections
- Networked Privileged Accesses
- Prevent Discovery of Systems Components
- Automated Enforcement of Protocols Formats
- Fail Secure
- Block Communication from Non-Organizationally Configured
- Dynamic Isolation and Segregation
- Isolation of Systems Components
- Separate for Connecting to Different Security Domains
- Disable Sender Feedback on Protocol Validation Failure
- Personally Identifiable Information
- Unclassified National Security Systems Connections
- Classified National Security Systems Connections
- Unclassified Non-National Security System Connections
- Connections to Public Networks
- Separate Subnets to Isolate Functions

Elijah Montgomery

IA-5 Authenticator Management

- Password Based Authentication
- Public Key-Based Authentication
- In Person or Trusted External Party Registration
- Automated Support for Password Strength
- Change Authenticators Prior to Delivery
- Protection of Authenticators

- No Embedded Unencrypted Static Authenticators
- Multiple Systems Accounts
- Federated Credential Management
- Dynamic Credential Binding
- Biometric Authentication Performance
- Expiration of Cached Authenticators
- Managing Content of PKI Trust Stories
- GSA-Approved Products and Services
- In Person or Trusted External Party Authenticator Issuance
- Presentation Attack Detection for Biometric Authenticators
- Password Managers

SC-8 Transmission Confidentiality

- Cryptographic Protection
- Pre and Post Transmission Handling
- Cryptographic Protection for Message Externals
- Conceal or Randomize Communications
- Protected Distribution System

Malik Douglas

IA-2 Identification And Authentication

- Privileged Accounts
- Local Access to Privileged Accounts
- Local Access to Non-Privileged Accounts
- Individual Authentication with Group Authentication
- Access to Accounts Separate Device
- Network Access to Non-Privileged Account - Separate Device
- Access to Accounts – Replay Resistant
- Network Access to Non-Privilege Accounts – Replay Resistant
- Single Sign On
- Remote Access – Separate Device
- Acceptance of PIV Credentials
- Out of Band Authentication

AC-23 DATA MINING PROTECTION

- No Control Enhancements

REMOTE ACCESS (AC-17)

SnowBe likely has a hybrid or remote workforce, making remote access control critical to secure company resources, prevent unauthorized access, and ensure secure connections for remote employees or contractors.

IDENTIFICATION AND AUTHENTICATION (IA-2)

Identification and authentication are foundational to ensuring that only authorized users can access systems and data. This is a critical control for protecting sensitive business information and maintaining the integrity of SnowBe's systems.

AUTHENTICATOR MANAGEMENT (IA-5)

Effective management of authenticators (passwords, tokens, etc.) is key to ensuring the security of user identities and preventing unauthorized access through weak or compromised credentials.

SECURITY AND PRIVACY ATTRIBUTES (AC-16)

Defining and managing security and privacy attributes for systems ensures that access is granted only based on clearly defined roles and security policies. This control is essential for enforcing SnowBe's security posture.

DATA MINING PROTECTION (AC-23)

Preventing unauthorized data mining is crucial for protecting sensitive business data and ensuring compliance with privacy regulations, especially as SnowBe might handle customer data.

BOUNDARY PROTECTION (SC-7)

Boundary protection prevents unauthorized access to SnowBe’s internal network from external sources, which is crucial for protecting against cyberattacks and data breaches.

TRANSMISSION CONFIDENTIALITY (SC-8)

Protecting data during transmission ensures that sensitive information is not exposed to potential interception. This is particularly important for a company like SnowBe that may transmit sensitive business and customer data.

CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT (SC-12)

Managing cryptographic keys properly is essential for maintaining the confidentiality and integrity of sensitive information, especially if SnowBe uses encryption for data at rest or in transit.

CRYPTOGRAPHIC MODULE AUTHENTICATION (IA-7)

Ensuring that cryptographic modules are properly authenticated is important for SnowBe’s security infrastructure to prevent the use of compromised or unauthorized cryptographic systems.

SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (SI-7)

Ensuring the integrity of software, firmware, and data is crucial to prevent malicious alterations or attacks that could undermine SnowBe's business systems.

INFORMATION IN SHARED SYSTEM RESOURCES (SC-4)

Shared systems and resources need to be properly secured to ensure that confidential information is not accessible by unauthorized users or entities.

MEDIA SANITIZATION (MP-6)

Ensuring that media is properly sanitized before disposal prevents unauthorized access to sensitive data, particularly when hardware is being decommissioned or recycled.

MEDIA TRANSPORT (MP-5)

Ensuring secure transport of media is crucial to prevent unauthorized access during data transfers, especially when transferring sensitive business or customer information between sites.

ACCESS CONTROL FOR TRANSMISSION (PE-4)

Controlling access to transmission lines and communications infrastructure ensures that only authorized users can access SnowBe's communication channels and prevents data leaks.

CRYPTOGRAPHIC PROTECTION (SC-13)

This ensures that cryptographic protection mechanisms are robust and effective for safeguarding SnowBe’s sensitive information, particularly data at rest or in transit.

PUBLIC KEY INFRASTRUCTURES CERTIFICATES (SC-17)

Managing public key infrastructure (PKI) and certificates is important for secure communications and ensuring trust between SnowBe's systems and external parties.

SECURE NAME/ADDRESS RESOLUTION SERVICE (SC-20)

Secure DNS and address resolution prevent man-in-the-middle attacks, which is critical for ensuring secure communications across SnowBe's network.

PROTECTION OF INFORMATION TEST (SC-28)

Protecting information during testing is essential to ensure that vulnerabilities are not introduced or exploited in SnowBe’s operational systems.

OUT OF BAND CHANNELS (SC-37)

Securing out-of-band communication channels prevents unauthorized interception of data and is critical for systems where communication outside the main network is needed.

SYSTEM BACKUP (CP-9)

Regular backups are essential for disaster recovery and business continuity. Ensuring data is regularly backed up protects SnowBe from data loss due to hardware failures or cyberattacks.

COMPONENT DISPOSAL (SR-12)

Proper disposal of system components prevents data leaks or breaches, especially when hardware containing sensitive data is decommissioned or discarded.

Standards and Procedures

Exceptions/Exemptions

Requests for exceptions or exemptions to this security plan must be submitted in writing using the official Security Exception Request Form, which is available from the IT department. The request must clearly outline the justification for the exception, including the business need or operational challenge that necessitates the deviation. It must also detail any associated risks and propose compensating security controls to mitigate those risks.

Requests should be directed to the IT Director, who holds the authority to review and approve or deny the request. In certain cases, the IT Director may escalate the request to executive leadership if broader organizational impact is anticipated.

Approved exceptions will be granted for a defined time period, typically not exceeding 90 days unless otherwise justified. Each exception is subject to review and renewal to ensure continued relevance and to minimize risk exposure. This structured process ensures security remains a priority while allowing flexibility to support critical business operations.

Version History Table

Version	Date	Description
1.0	April 07, 2025	Initial document creation
2.0	April 09, 2025	Minor updates and citation review
2.1	April 21, 2025	Revise Master Plan
2.2	April 28, 2025	Week 3 updates

Citations

International Organization for Standardization. (2022). *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2022).* https://www.iso.org/standard/82875.html

Maryland Department of Information Technology, Office of Security Management. (n.d.). *Cybersecurity framework guidebook.* https://doit.maryland.gov/cybersecurity/Documents/CSF-Guidebook.pdf

Clarkson University, Office of Information Technology. (n.d.). *Information security standards (OM-912).* https://bookstack.clarkson.edu/books/operations-manual/page/om-912-information-security-standards

ChatGPT. (2025). *Access control policy explanation for IT management.* In response to the prompt: "Can you write a paragraph for each of the selected policy items assigned to my peers for an IT manager to understand the purpose of each item policy."

ChatGPT. (2025). *Data retention policy explanation for IT management.* In response to the prompt: "Can you write a paragraph for each of the selected policy items assigned to my peers for an IT manager to understand the purpose of each item policy."

ChatGPT. (2025). *Encryption policy explanation for IT management.* In response to the prompt: "Can you write a paragraph for each of the selected policy items assigned to my peers for an IT manager to understand the purpose of each item policy."

ChatGPT. (2025). *Firewall policy explanation for IT management.* In response to the prompt: "Can you write a paragraph for each of the selected policy items assigned to my peers for an IT manager to understand the purpose of each item policy."

ChatGPT. (2025). *Incident response policy explanation for IT management.* In response to the prompt: "Can you write a paragraph for each of the selected policy items assigned to my peers for an IT manager to understand the purpose of each item policy."

ChatGPT. (2025). *Password management policy explanation for IT management.* In response to the prompt: "Can you write a paragraph for each of the selected policy items assigned to my peers for an IT manager to understand the purpose of each item policy."

Payment Card Industry Security Standards Council. (2022). Payment card industry (PCI) data security standard: Requirements and security assessment procedures (Version 4.0).