SNOWBE ONLINE SECURITY PLAN

Jedson Jerume

Version 2.0 Date August 29th 2025

Table of Contents

Section 1: Introduction

The SnowBe Online Security Plan clearly defines security standards and procedures for ensuring the confidentiality, integrity, and availability of all information systems and resources managed by SnowBe's information technology department from unauthorized access, alteration, damage, intrusion, and misuse. As the company is now becoming public, it is important to have security to protect its digital assets, customer data, and company operations. The laid-back culture that was used to contribute to SnowBe's success must now change.

This plan will include definitions of key terms used in this plan and related documents.
Roles and responsibilities of key personnel and departments within SnowBe.
Descriptions and references to the standards and procedures for:

- Information System Documentation
- Secure System Management
- Technology Acquisitions
- Secure system and data access
- System and data integrity maintenance
- Data classification and use restrictions
- Risk management practices
- Security incident response and remediation
- Security awareness training
- Audit and compliance activities

To clearly define IT security standards and procedures that protect the confidentiality, integrity, and availability of all IT systems, data, and resources under SnowBe Online's Information Technology Services. (Depaw)

Section 2: Scope

This IT Security Plan applies to all SnowBe employees, third-party agents, and any other affiliates who are authorized to access SnowBe's data and IT resources. (Howard University) It also includes any personnel who interact with SnowBe's information systems, whether on-premises or cloud-hosted (AWS). It includes all servers, desktops, laptops, point-of-sale systems, and network devices across SnowBe's offices and storefronts globally.

Section 3: Definitions

formatted in a manner that would allow the user the ability to quickly scan the list and locate the term in question. Here are some examples of how this can be accomplished by:
Placing the term in bold and the definition in normal text. Placing the term (in bold) on one line and the definition below it. Utilizing a subtle shading of every other term.
etc.

Section 4: Roles & Responsibilities

Defines specific duties for various roles, including Executive, Administrative, and other employees with access to information resources:

- Chief Information Officer:

At SnowBe Online, the CIO is the visionary leader of all information technology initiatives, aligning digital innovation with the company's rapid growth and laid-back yet ambitious culture. As the company transitions to the public market, the CIO ensures IT operations support business scalability, data integrity, and regulatory compliance while preserving the brand's unique customer connection. (Infosec Institute)

- Director of Information Technology:

  The Director of IT at SnowBe Online manages day-to-day operations across the company's tech infrastructure, supporting everything from customer experience systems to backend logistics. This role bridges technical strategy and team coordination, ensuring the technology environment remains reliable, secure, and agile to match the company's fast-paced growth. (Infosec Institute)

- Information Security Workgroup (ISW):

  The ISW is a cross-functional team within SnowBe Online that brings together stakeholders from IT, marketing, legal, and operations to guide and promote security practices. Their role is vital in protecting customer trust and company assets by evaluating risks, shaping policies, and supporting a security culture across departments. (Infosec Institute)

- Office of Information Security (OIS):

  The Office of Information Security shows its commitment by developing and implementing good internal controls as well as ensuring the promotion and awareness of IT requirements and plans throughout the Brand. SnowBe Online's strategic vision is linked with the IT department's goals and objectives, ultimately assuring that the brand meets customer and legal requirements while undergoing continual improvement. (Michigan Technological)

- System Administrator (SA):

  The System Administrator ensures the secure and smooth operation of SnowBe Online's network and server infrastructure. From managing user accounts to applying system updates, the SA is critical in keeping business systems—especially e-commerce platforms—running efficiently and protected against disruptions or cyber threats. (Infosec Institute)

Section 5: Statement of Policies, Standards and Procedures

Policies

1. Patch Management Policy

Summary: This policy ensures all SnowBe systems—including AWS servers, endpoints, and POS devices—are regularly updated with security patches to reduce vulnerabilities, maintain compliance, and protect customer data.

2. Cybersecurity Maturity Policy

Summary: This policy establishes SnowBe's framework for assessing and improving cybersecurity maturity levels, aligning with CIS Controls to prioritize risk reduction and strengthen resilience across global operations.

3. Secure Software Development Life Cycle (SDLC) Policy

Summary: This policy integrates security into every phase of SnowBe's SDLC to safeguard applications, prevent misuse of sensitive data, and ensure secure, compliant software development and deployment.

Standards and Procedures

Section 6: Exceptions/Exemptions

Any request for an exception/exemption to any policy, standard, or procedure must: (Davidson College)

- Be submitted in writing to the Director of IT or OIS
- Include a clear justification for the request and any compensating controls in place.
- Be reviewed and approved by the Director.
- Include a defined expiration date (no longer than 12 months) after which the exception must be re-evaluated or retired.
- Exceptions do not guarantee approval and may be denied if deemed a critical risk.
- All requests for an Exception/Exemption in policy will be archived even if the request is denied.

Section 7: Version History Table

Version	Date	Description
2.0	August 29th 2025	Template Creation

Citations

https://www.davidson.edu/offices-and-services/technology-innovation/it-guidelines-policies/information-systems-security-policy

https://www.depauw.edu/it/policies/information-security-plan/

https://www.infosecinstitute.com/resources/professional-development/what-does-a-system-administrator-do-and-how-to-become-one/

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://gta-psg.georgia.gov/psg/cybersecurity-capability-maturity-model-ss-20-001

https://www.roehampton.ac.uk/globalassets/documents/corporate-information/policies/cyber-security-policies/patch-management-policy.pdf/

https://www.esecurityplanet.com/compliance/patch-management-policy-template/
https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2