SNOWBE ONLINE SECURITY PLAN

Group Member Names:

Baez Hernandez Paola
Books Megan
Mendoza-Paz Cristian
Granado Erica

Version #1 Date 01/09/2025

Table of Contents

Section 1: Introduction

An overview of SnowBe Online's Security Management System for the purpose of compliance, response, and recovery. A comprehensive listing of the practices for prevention, mitigation, and security ensures a strategic approach is in place for a quick response while meeting legal and necessary obligations.

Section 2: Scope

This security plan applies to all information systems and assets managed by SnowBe Online. This includes but is not limited to, the AWS-hosted platform, internal workstations, on-premise and cloud-based servers, and the IT infrastructure of physical retail storefronts across the U.S. and Europe. The plan applies to all employees and third-party service providers who access or interact with SnowBe Online's information systems. Additionally, this plan also extends to all sensitive customer data, including customer personal information and payment card details, in compliance with applicable regulatory standards such as PCI DSS. The plan's scope extends to the entirety of SnowBe Online's operations.

Section 3: Definitions

1. Access Control:

This is how SnowBe Online decides what gets access to and can see or use certain information or systems. It has a locked door to which only certain employees have the key. For example, employees in the sales department might have access to customer orders but not the accounting information. This helps ensure sensitive stuff doesn't get into the wrong hands.

2. Confidential Data:

Confidentiality is very necessary and crucial for data and any company's sensitive information. This means keeping everything safe. For SnowBe Online, it means customers' credit card numbers, personal information, and any shopping history.

3. Encryption:

Encryption is putting data in secret code mode, so only people with the right key can read it. SnowBe online benefits from it to protect information when stored on the computer, for example, a database, or being sent over to the internet, for example, when shopping online. This means if someone tries to steal any information, they won't be able to make sense of it unless they have the right key.

4. PCI Compliance:

PCI Compliance is a set of rules that businesses are mandated to follow and in order to protect their customer' credit card information. These rules are made to ensure that when customers pay online,

their information is protected from hackers. SnowBe Online being PCI compliant means they must follow these security rules when handling payment information to prevent data breaches or any fraud.

5. Virtual Private Network:

VPN is a secure way to connect to the company's network over the internet, especially when working remotely. This keeps things safer. It's like a tunnel between your computer and the company's servers. This will ensure one spy on your personal activity and steals your data while working from home.

Section 4: Roles & Responsibilities

SnowBe Online's Information Security Plan states, "Individuals authorized to access the company's data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved by SnowBe Online's Policy Committee, and maintained by the Information Security Office." These roles and responsibilities are defined as follows:

Chief Information Officer:

- Responsible for the company's security program and ensuring that all policies, procedures, and standards are developed, implemented, and maintained.
- Ensures that company policies are developed and enforced following this policy.
- Conducts an annual review to ensure program effectiveness and alignment with business goals.

Data Custodian:

- Responsible for documenting and reporting how data is processed, stored, and transmitted by the company and third-party agents.
- Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of company data.
- Understanding and reporting security issues and their impact on confidentiality, integrity, and availability of company data.

General Users:

- Adhering to policies, guidelines, and procedures about the protection of company data.
- Reporting suspected vulnerabilities in confidentiality, availability, or integrity of company data to ISO.

Information Security Officer:

- Oversee the implementation and development of SnowBe's information security program.
- Establish security objectives that align with business goals and regulations.
- Develop, maintain, and enforce security policies, procedures, and standards related to online operations, on-premise servers, and employee devices.
- Create and manage an incident response plan.

- Oversee system updates, configurations, and vulnerabilities.

Management Team:

- Advocate for security awareness to ensure employees follow best practices.
- Provide resources to implement the company's information security program.
- Ensure all business operations comply with security standards and regulations.

Technical Consultant:

- Assist in applying technical updates like firmware, antivirus, patching, etc.
- Establish strict access controls to ensure data is restricted based on employee roles.
- Provide regular progress reports to the management team.
- Document implemented changes to maintain a comprehensive security configuration record.

Section 5: Statement of Policies, Standards and Procedures

Policies

Standards and Procedures

Section 6: Exceptions/Exemptions

Exceptions / Exemptions Request Process

How: Placing a request for the form through the company's personnel website.

Why: There are drop-down buttons on the form that let you write in the reason for asking for an exception or exemption if one is not given and can't be chosen.

Who has authority for approval:
An approval hierarchy will be in place in accordance with the request. Including the level of access and the nature of exception/exemption.

This includes the management team
Human Resources

Section 7: Version History Table

Version	**Date**	**Description**
V.01	01-09-2025	Initial Security Plan Template for SnowBe Online

Citations

Introduction

ComplianceWire. (2024, June 24). *SAMPLE SECURITY PLAN*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.compliancewire.com/EduFlexCourses/Courses/C_769_4247/Assets/lang_1/jobaids/sample_security_plan.pdf https://www.compliancewire.com

Scope:

(2011, October 13). Michigan Technological University. https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

Definitions:

Occidental College. (n.d.). Information Security Plan (Definitions). Occidental College. https://www.oxy.edu/policy-directory/information-security-plan?utm_source

Grimmick, R. (2024, November 13). What is a security policy? Definition, elements, and examples. Varonis. https://www.varonis.com/blog/what-is-a-security-policy

Roles and Responsibilities:

Piersol, J. F. (2019, November 1). Howard University Information Security plan. https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf

Eastern Kentucky University. (2019, February 22). *Administrative regulation: 11.2.4ADR*. Information Technology. https://drive.google.com/file/d/1gF2HPW4NiI1nnCmELBx_qTUMvzvYsz2z/view

Exceptions/Exemptions

Nguyen, T. (2019, January 24). *Exception Management Policy – Best Practices*. Information Security Program. https://informationsecurityprogram.com/