SNOWBE ONLINE SECURITY PLAN

**Donald Doss  
Hernandez Gabriel  
Michael Kohronas  
Xavier Rivera Maysonet  
Michael Vazquez**

**<Security Plan>**

**Version #1**

**Date 10/2024**

**Table of Contents**

[Section 1: Introduction 2](#_Toc144567015)

[Section 2: Scope 2](#_Toc144567016)

[Section 3: Definitions 2](#_Toc144567017)

[Section 4: Roles & Responsibilities 2](#_Toc144567018)

[Section 5: Statement of Policies, Standards and Procedures 2](#_Toc144567019)

[Policies 2](#_Toc144567020)

[Standards and Procedures 2](#_Toc144567021)

[Section 6: Exceptions/Exemptions 2](#_Toc144567022)

[Section 7: Version History Table 2](#_Toc144567023)

[Citations 2](#_Toc144567024)

# Section 1: Introduction

The purpose of this security plan is to safeguard the confidentiality, integrity, and availability of SnowBe Online’s data and IT resources. This document outlines policies and practices designed to address the evolving threat landscape while supporting the company’s laid-back culture.

This plan ensures SnowBe’s systems meet legal, ethical, and operational standards, providing a secure environment for employees, customers, and vendors. It emphasizes proactive measures, including threat modeling, software patch management, and regular security maturity assessments, to build and maintain trust with stakeholders.

# Section 2: Scope

This plan applies to all employees, contractors, and external partners who use or manage SnowBe Online’s IT resources. It covers on-premises and cloud environments (AWS), including desktops, mobile devices, servers, and third-party applications such as WordPress.

All systems, including customer data, transaction records, and business-critical applications, fall under the scope of this plan. Compliance with these policies is mandatory to ensure the security of information held, transmitted, or processed on behalf of SnowBe Online.

This plan governs the use, storage, and protection of:

* Data across media (paper, digital, or verbal).
* Company devices and infrastructure, including mobile devices and servers.
* Customer and business information, including PCI-compliant payment data.

# Section 3: Definitions

**Critical Patch -** A high-priority update that addresses severe vulnerabilities requiring immediate action.

**Maturity Levels -** Security maturity is often measured using established frameworks such as NIST Cybersecurity Framework (CSF), Capability Maturity Model Integration (CMMI), or the Cybersecurity Maturity Model Certification (CMMC). These frameworks define maturity levels, from basic (ad-hoc) to advanced (optimized and proactive).

**Non-Critical Patch -** An update aimed at minor bug fixes or performance improvements, not urgent in nature.

**Patch -** A software update that resolves vulnerabilities, improves performance, or fixes bugs.

**Secure System Development Life Cycle (SSDLC) -** Security requirements and tasks that must be considered and addressed within every system, project, or application that is created or updated to address a business need.

**Security Maturity -** A measure of an organization’s ability to manage security risks effectively, ranging from ad-hoc responses to structured, optimized, and proactive practices.

**System Development Life Cycle (SDLC) -** A structured process that encompasses the planning, design, development, testing, deployment, operation, and eventual decommissioning of a system.

**Threat Modeling -** A security process to identify, prioritize, and mitigate potential threats to a system.

# Section 4: Roles & Responsibilities

**All Employees, Contractors, or Interns -** Follow security policies, complete training, and report any suspicious activity.

**Chief Information Security Officer (CISO) -** Leads security maturity assessments, ensures alignment of all security initiatives, and oversees the integration of security within SDLC phases.

**Project Managers -** Ensure that security tasks, including patching, are integrated into project timelines. They coordinate with IT Operations to reduce disruptions during updates.

**Developers -** Apply secure coding practices and support patching efforts to ensure software compatibility and mitigate risks.

**Security Team:** Conduct threat modeling and vulnerability assessments, and validate post-patch security.

**IT Operations:** Monitor patch releases, deploy updates, and maintain system stability while tracking compliance and providing reports to management.

# Section 5: Statement of Policies, Standards and Procedures

## Policies

## **System Development Life Cycle (SDLC) Policy -** Security tasks are embedded into each SDLC phase, including planning, development, testing, deployment, and disposal. Threat modeling is used during design to identify and mitigate potential risks early in the process.

## **Software and System Patch Management Policy -** Critical patches are applied within 72 hours, and non-critical patches within 30 days. IT Operations tests patches before deployment to ensure stability, and the Security Team validates that vulnerabilities are resolved post-patching.

## **Security Maturity Policy -** SnowBe follows the Plan-Do-Check-Act (PDCA) model to ensure continuous improvement. Regular assessments and external audits guide improvements, and employee security training is mandatory. Progress is tracked using KPIs, including patch compliance and incident response times.

## Standards and Procedures

# Section 6: Exceptions/Exemptions

# Exceptions to this policy will be considered on a case-by-case basis and **do not guarantee**

# **approval**. To request an exception, please submit a written request to the **IT Director** outlining the

# following:

# **How to Request Exceptions/Exemptions?**

# To request an Exception or Exemption from a policy that is in place please message

# ITDirector@SnowBe.com with the following format:

# What Exception/Exemption are you requesting?

# Why are you requesting this Exception?

# How long are you requesting this Exception/Exemption for?

# The **IT Director**, in consultation with relevant stakeholders, will review the request and determine if

# an exception can be granted. **The decision will be based on the potential impact on security, the**

# **justification provided, and the availability of alternative secure solutions.**

# Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

# **Enforcement –** The failure to comply with policies, standards, or procedures will result in a warning

# or disciplinary action depending on the severity of the infraction.

# Section 7: Version History Table

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | 10/27/2024 | Initiation/Finalization |
|  |  |  |
|  |  |  |
|  |  |  |

# Citations

<https://www.salisbury.edu/administration/general-counsel/policies/section_X/X-27.00-SU-SDLCPolicy.pdf>

<https://its.ny.gov/secure-system-development-life-cycle-standard>