SNOWBE ONLINE Policy# CMMC Security Maturity Policy

Humberto Gonzalez

Version # 1.0

DATE: November 19, 2024

<Template Policy> – V 1.0
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Humberto Gonzalez
DATE: 11-19-2024

Table of Contents

Purpose

This policy aims to develop a standardized approach for assessing and improving SnowBe Online's security maturity. By systematically analyzing security procedures, finding gaps, and implementing improvements, this policy strives to protect customer data, satisfy regulatory compliance, and maintain a strong cybersecurity posture.

Scope

This policy applies to all employees, contractors, vendors, and stakeholders involved in the implementation, maintenance, or assessment of SnowBe Online's security measures. It includes all IT systems, data, and procedures, such as our AWS-hosted website, storefront operations in the United States and Europe, and corporate endpoints.

Definitions

Security Maturity: The level of development and effectiveness of SnowBe's cybersecurity practices and controls.

Roles & Responsibilities

- Employees: Comply with security policies and participate in awareness programs.
- Chief Information Security Officer (CISO): Oversees the security maturity assessment and ensures alignment with organizational goals.
- IT Operations Team: Implements and documents security measures for corporate and AWS-hosted environments..
- Risk Management Team: Conducts risk assessments for e-commerce and payment systems, including PCI DSS compliance.

Policy

1. Assessment Framework:
   - SnowBe Online will use the Cybersecurity Capability Maturity Model (C2M2) as a framework to evaluate and improve security processes.
   - Annual assessments will be conducted or following significant changes in technology, business operations, or regulatory requirements.

2. Defined Maturity Levels:

The organization will evaluate security maturity across key areas:

- Access Control (AC)

- Incident Response (IR)
- Risk Management (RM)
- System and Information Integrity (SI)
- Configuration Management (CM)
- Audit and Accountability (AU)
- System and Communications Protection (SC)
- Access Control (AC)
- Awareness and Training (AT)

3. Gap Analysis:
   - Identified security gaps will be documented in a report that includes related risks, potential consequences, and suggested actions.

4. Continuous Improvement:
   - Create and implement improvement strategies with specific dates and responsibilities.
   - Conduct quarterly evaluations to track success and adjust plans as needed.

5. Metrics and Reporting:
   - Key performance indicators (KPIs) such as incident reaction times, patch deployment rates, and security training completion rates will be monitored to assess progress.

6. Awareness and Training:
   - Employees will receive regular security awareness training to help limit the risks associated with human error, such as phishing attacks and misconfiguration.

7. Compliance:
   - SnowBe Online will comply with legislation and standards such as GDPR, PCI DSS, SOX, and CCPA to protect consumer data and retain confidence.

8. Review and Updates:
   - This policy will be reviewed and updated on an annual basis, or as appropriate, to reflect new cybersecurity threats, business developments, or regulatory updates.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	11/19/2024	Humberto Gonzalez	TBD	Created the initial version of the Security Maturity Policy for SnowBe Online.

Citations

C2M2- C2M2 Version 2.1 June 2022

CCPA- California Consumer Privacy Act Regulations

CMMC Resources- CMMC Resources & Documentation

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

GDPR- General Data Protection Regulation (GDPR) – Legal Text

PCI DSS- PCI_DSS-QRG-v4_0.pdf

Purpose/Introduction- Michigan Technological University Information Security Plan (mtu.edu)

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)

Enforcement- Sample Detailed Security Policy (bowiestate.edu)