SNOWBE ONLINE

Policy# SM 01

Security Maturity

Chris Stevens

Security Maturity

Version # 1.0

DATE:

Security Maturity – V 1.0
Status: ✠ Working Draft □ Approved □ Adopted
Document owner: Chris Stevens
DATE: 10-28-2025

Table of Contents

Purpose

The purpose of this Security Maturity Policy is to establish a framework for systematically assessing, improving, and maintaining the cybersecurity posture of SnowBe Online. This policy outlines the company's commitment to continuously enhancing its security controls, processes, and technologies to protect its assets, customer data, and brand reputation from evolving threats. It serves to guide the implementation of security measures based on a maturity model, ensuring that the company progresses from a reactive to a proactive and well-managed security state.

Scope

This policy applies to all employees, contractors, consultants, and third-party vendors who have access to SnowBe Online’s systems, data, and network infrastructure. This includes, but is not limited to, corporate desktops, laptops, mobile devices, on-premise servers, AWS cloud assets, network devices, and all applications used for business operations, such as the company website, customer relations management (CRM), and order management systems. This policy covers all physical locations, including the main office in Los Angeles and all storefronts in the U.S. and Europe, as well as remote access to company resources.

Definitions

Security Maturity Model
A framework used to measure an organization's capability and effectiveness in managing cybersecurity risks. It typically uses a scale (e.g., from 1 to 5) to rate the sophistication of security processes and controls.

Technical Controls
The security measures implemented in hardware, software, or firmware to protect information systems and data. Examples include firewalls, intrusion detection systems, antivirus software, and access control mechanisms.

NIST Risk Management Framework (RMF)
A structured approach to managing security and privacy risks, used by the technical consultant to analyze SnowBe Online's risk posture.

PCI Compliance
A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Firmware
A specific class of computer software that provides the low-level control for a device's specific hardware.

Vulnerability
A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Roles & Responsibilities

IT Director/IT Management
Responsible for overseeing the implementation and enforcement of this policy. They will approve risk acceptance memos and guide the Information Security Office on policy exceptions.

Information Security Office
Responsible for approving policy exceptions , maintaining documentation of approved exceptions, and performing periodic reviews. They will also manage the risk acceptance process.

IT Department
Responsible for investigating suspected policy violations , documenting approved exceptions, and ensuring the policy is implemented across the company's systems.

All Employees
Required to comply with the policy. Violations may result in disciplinary action, including suspension of access privileges.

Technical Consultant
Responsible for identifying initial security gaps and recommending controls based on the NIST 800-53 r5 framework.

Policy

SnowBe Online is committed to a continuous improvement model for its cybersecurity posture. The company will implement a Security Maturity Model to guide this process, which will include the following phases:

1. Initial Assessment: An initial assessment has been performed by a technical consultant, which identified key areas for improvement, including outdated firmware, unpatched systems, and a lack of granular access controls.

2. Implementation of Foundational Controls: Based on the assessment, the company will prioritize the implementation of foundational security controls. This includes:

    a) Updating firmware on all network devices.
    b) Applying patches and updates to all PCs and Windows servers to the latest versions.
    c) Updating antivirus and backup software.
    d) Securing on-premise servers in a locked area.
    e) Updating the WordPress shopping cart.

3. Process and Access Control Enhancements: SnowBe Online will implement processes to manage and restrict access to company data.

    a) The access management system will be refined to ensure employees only have access to the data and applications necessary for their roles.

b) Mobile devices must be reviewed and approved by the IT department before being granted access to company data.
c) Login audit records will be saved for at least three months, with older records archived to a cloud storage facility.

4. Compliance and Ongoing Improvement: The company will implement all required PCI compliance items to secure credit card transactions. The security maturity model will be reviewed periodically to ensure continuous improvement and adaptation to new threats.

Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not constitute a permanent change to the policy.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Enforcement

Enforcement
SnowBe Online takes the enforcement of this (Policy name) seriously to protect its systems, data, and customers.

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment, contract cancellation, and/or legal action.

The penalties will include the following components:

Monitoring and Auditing
SnowBe Online reserves the right to monitor, log, and audit all system and network activity to ensure compliance with this policy. Users should have no expectation of privacy when using company-owned systems or accessing company data.

Incident Investigation
Suspected policy violations will be investigated promptly by the IT department, Human Resources, and other relevant stakeholders. Users are expected to cooperate fully during any investigation.

Corrective Action
If a violation is confirmed, corrective actions will be taken based on the severity and nature of the breach. This may include revocation of access, mandatory training, written warnings, or other disciplinary measures as outlined in the employee handbook.

Legal Consequences
Activities that are illegal under local, state, or federal law may be reported to the appropriate authorities. This includes unauthorized access, data breaches, or misuse of customer financial information.

Appeals Process
Individuals who believe they were unfairly penalized for a policy violation may appeal the decision to management or HR following internal dispute resolution procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-28-2025	Chris Stevens	CEO	Security Maturity Policy Creation

Citations

Verizon
https://www.verizon.com/business/resources/articles/s/cyber-security-maturity-models-and-how-to-implement-one/
Purpose, Scope, Definitions, Roles & Responsibilities.

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, but as a group we revised the verbiage.

Policy Template
https://www.sans.org/information-security-policy/
Exceptions/Exemptions