SNOWBE ONLINE Policy#

Security Maturity Policy

Your name: Jedson Jerume

Security Maturity Policy -

Version #2 DATE:08/28/25

Table of Contents

Purpose

The purpose of this policy is to establish a structured approach for SnowBe to measure, evaluate, and improve the maturity of its cybersecurity practices. By adopting a cybersecurity maturity model, SnowBe can baseline its current security capabilities, identify gaps, and create a roadmap for continuous improvement. This framework not only provides a consistent method for assessing SnowBe's technical and organizational readiness but also serves as a guide to achieving higher levels of maturity. Strengthening cybersecurity maturity helps protect customer data, reduces operational risk, supports compliance requirements (e.g., PCI DSS, GDPR), and enhances customer trust in SnowBe's global operations.

Scope

This policy applies to all SnowBe business operations, including:

- **Corporate Headquarters in Los Angeles** (servers, desktops, and laptops used for administration, accounting, and customer support).
- **Storefronts in the U.S. and Europe** (POS systems, desktops, and devices used for sales).
- **AWS-hosted platforms and applications** supporting SnowBe's e-commerce website and customer database.
- **All employees, contractors, consultants, and third-party service providers** with responsibilities for managing, supporting, or securing SnowBe's IT assets.

This policy encompasses enterprise-wide systems, applications, and infrastructure—whether developed in-house or managed by third parties—that process, store, or transmit SnowBe business and customer data.

Definitions

Cybersecurity Maturity: The level of an organization's capability to protect, detect, respond to, and recover from security threats, measured against defined stages of improvement.

Baseline Assessment: The initial measurement of SnowBe's cybersecurity posture to establish the current maturity level.

Maturity Levels: Standardized benchmarks (e.g., Level 1–Initial, Level 2–Developing, Level 3–Defined, Level 4–Managed, Level 5–Optimized) used to evaluate progress.

Security Controls: Technical, administrative, and physical safeguards that reduce security risks to SnowBe systems and data.

Continuous Improvement: Ongoing efforts to enhance security processes and adapt to evolving threats.

Roles & Responsibilities

Executive Management:
Provide strategic direction, approve budgets for security improvements, and review maturity assessment results.

Project Manager for IT Security (Karen):
Acts as the Security Maturity Authority. Coordinates maturity assessments, ensures corrective actions are prioritized, and reports results to management.

IT & Cybersecurity Consultant (Brad):
Supports technical assessments, evaluates SnowBe's environment against maturity standards, and provides recommendations for improvement.

System Administrators / IT Staff:
Implement security controls, maintain patching and monitoring processes, and provide evidence for maturity assessments.

Employees (All Users):
Follow security awareness training, comply with SnowBe's policies, and report suspicious activity or potential vulnerabilities.

Third-Party Vendors / Partners:
Ensure systems and services provided to SnowBe meet defined maturity requirements and participate in audits if required.

Policy

The SnowBe Cybersecurity Capability Maturity Model is a tool used to develop, assess, and refine SnowBe's cybersecurity program. The model provides a framework to evaluate, rate, and score SnowBe's maturity level annually, aligned with the **Center for Internet Security (CIS) 20 Critical Security Controls**.

SnowBe will conduct an annual maturity self-assessment using a **Cybersecurity Maturity Questionnaire**, covering AWS-hosted systems, on-premises servers, POS devices, laptops, and network infrastructure. The results will guide prioritization of improvements and will also influence SnowBe's cyber insurance premiums, deductibles, and vendor risk posture.

Failure to complete the annual assessment will be treated as operating at **Maturity Level 0**, which places SnowBe at the highest risk score tier.

Maturity Level Details (SnowBe)

- **Maturity Level 0 (None):** No formal processes. SnowBe operates reactively, with ad hoc fixes and no consistent controls.
- **Maturity Level 1 (Initial):** Processes are informal and inconsistent. Security depends heavily on individual effort (e.g., Brad implementing AV, firewall, and backups).
- **Maturity Level 2 (Repeatable):** SnowBe begins establishing repeatable processes such as documented patch management, access control (Active Directory), and backup schedules. Processes are tracked and followed but not yet standardized across all teams.
- **Maturity Level 3 (Defined):** Security processes are formally documented, understood, and enforced. Awareness training, risk management practices, and vendor oversight become part of SnowBe's culture.
- **Maturity Level 4 (Quantitatively Managed):** SnowBe applies metrics and monitoring to measure security effectiveness (e.g., RMM reports, vulnerability scanning, patch compliance dashboards). Security performance is predictable.
- **Maturity Level 5 (Optimized):** Continuous improvement is embedded into SnowBe's culture. Lessons learned from incidents and assessments drive improvements. Security integrates into business strategy and innovation.

Cyber Insurance Risk Tiers (SnowBe)

Maturity Level	CIS Controls Coverage	Risk Score	SnowBe Context
Level V (Optimized)	CIS Controls 1–20	**1.0**	Fully integrated cyber resilience across AWS, POS, HQ, and storefronts.
Level IV (Managed)	CIS Controls 1–19	**1.5**	Measured and tracked; near full coverage.
Level III (Defined)	CIS Controls 1–19	**2.0**	Documented, standardized processes in place.
Level II (Repeatable)	CIS Controls 1–6, 10, 17	**3.0**	**Target for SnowBe**: Basic processes exist (patching, access control, backups) and are consistently applied.
Level I (Initial/Informal)	CIS Controls 1–6, 10, 17	**4.0**	**SnowBe's current state**: AV, firewall, AD, and RMM are in place but still ad hoc.
Level 0 (None)	No processes	**5.0**	No controls in place; unacceptable risk posture.

Exceptions/Exemptions

SnowBe recognizes that certain cybersecurity maturity practices may not be fully implemented immediately due to technical limitations, budget constraints, or resource availability. Exceptions to this policy must be formally documented, justified, and approved by the **Project Manager for IT Security (Karen)**, who acts as the **Security Maturity Authority**.

Examples of exceptions include:

- **Unsupported Systems:** Legacy POS or on-premise systems that cannot meet newer CIS Control requirements.
- **Third-Party Dependencies:** Vendor-provided services where SnowBe cannot directly enforce maturity practices.
- **Resource Constraints:** Delayed implementation of specific CIS Controls due to staffing or budget limitations.

All exceptions must include:

1. The control or maturity requirement not being met.
2. The reason for the exception.
3. Any compensating controls or mitigation steps in place.
4. A timeline for review and re-evaluation.

Exceptions will be reviewed **quarterly** to determine whether the gap has been addressed, if mitigations remain effective, or if retirement/replacement of affected systems is required.

Enforcement

Compliance with the SnowBe Cybersecurity Maturity Policy is **mandatory**.

- **Employees:** Any employee or contractor who intentionally disregards maturity requirements (e.g., bypassing access control, ignoring training, or mishandling sensitive data) may face disciplinary action up to and including termination.
- **IT and Security Staff:** The performance of IT administrators, consultants, and staff will be evaluated in part on their ability to implement, maintain, and improve maturity processes. Repeated failure to meet requirements, falsified reports, or gross negligence may result in disciplinary action or termination.
- **Non-Compliant Systems:** Any device, server, or application that fails to meet maturity standards may be removed from SnowBe's production environment, segregated to a restricted network, or denied access to critical systems until compliance is restored.
- **Vendors and Third Parties:** Service providers that fail to meet agreed-upon maturity standards may face contract penalties, restricted access, or termination of services.

Enforcement ensures that SnowBe steadily improves its maturity level, reduces cyber risk, and maintains trust with customers, regulators, and business partners.

<Template Policy> – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Jedson Jerume
DATE: 08/28/25

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
SP2.0	August 28th 2025	Jedson Jerume	Jedson Jerume	security maturity policy update

Citations

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

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2