SNOWBE ONLINE Policy # SP-02: Security Maturity Policy

James Chapman

<SP-02 Security Maturity Policy>

Version # 1.0.0

Date 05/29/2025

Table of Contents

Purpose

The purpose of this Security Maturity Policy is to establish a formal framework for assessing, documenting, and continuously improving the cybersecurity maturity of SnowBe Online. This policy ensures that the organization's security posture evolves in alignment with business growth, regulatory requirements, and the changing threat landscape, supporting the confidentiality, integrity, and availability (CIA) of all information assets.

Scope

This policy applies to all SnowBe Online employees, contractors, and third-party vendors who have access to company information systems, data, and technology infrastructure. It covers all business units, IT systems, and critical security domains, including but not limited to Access Control, Risk Management, Audit & Accountability, Configuration Management, and Incident Response.

Definitions

- Security Maturity: The degree to which an organization's security processes are defined, managed, measured, and optimized.
- Maturity Model: A structured framework (e.g., CMMC, C2M2, NIST) used to assess and guide the advancement of security capabilities.
- Key Performance Indicators (KPIs): Metrics used to measure progress toward security maturity goals (e.g., patch compliance rate, incident response time).
- Continuous Improvement: An ongoing process of assessing, updating, and optimizing security controls and processes.

Roles & Responsibilities

- Chief Information Security Officer (CISO): Oversees the patch management program and ensures compliance with this policy.
- IT Manager: Coordinates patch identification, testing, deployment, and documentation; conducts regular audits.
- System Administrators: Responsible for timely patch application, system monitoring, and reporting exceptions.
- Employees: Must report observed vulnerabilities and comply with scheduled maintenance notifications.
- Third-Party Vendors: Required to follow SnowBe Online's patch management standards for any systems or applications they manage

Policy

1. Adoption of Maturity Model:
   SnowBe Online will use an industry-recognized security maturity model (e.g., CMMC, C2M2, or NIST) to assess and benchmark the organization's security posture annually.
2. Assessment & Documentation:
   - Conduct an annual security maturity assessment across all critical domains (e.g., Access Control, Risk Management, Audit & Accountability, Configuration Management, Incident Response).
   - Document the current maturity level for each domain using a five-level scale:
     - Level 1: Initial (ad hoc, undocumented)
     - Level 2: Managed (basic controls in place)
     - Level 3: Defined (standardized, documented)
     - Level 4: Quantitatively Managed (metrics-driven)
     - Level 5: Optimizing (continuous improvement).
3. Maturity Roadmap & Improvement:
   - Develop a 12-month roadmap to advance targeted domains to higher maturity levels based on business priorities and risk assessments.
   - Short-term (0-3 months): Address foundational controls (e.g., RBAC, vulnerability scanning).
   - Mid-term (3-6 months): Develop and document incident response plans, configuration baselines.
   - Long-term (6-12 months): Achieve target maturity levels, implement continuous training, and prepare for external certification if required.
4. Measurement & Reporting:
   - Track KPIs such as patch compliance rate, number of unauthorized access attempts, log review completion rate, and incident response time.
   - Report progress quarterly to executive leadership and update the maturity roadmap as needed.
5. Continuous Improvement:
   - Integrate lessons learned from incidents, audits, and assessments into the maturity roadmap.
   - Foster a culture of security-first thinking and continuous improvement across all teams.

Exceptions/Exemptions

Requests for exceptions to this policy must be submitted in writing to the CISO, including justification and proposed compensating controls. All exceptions require risk assessment and executive approval, and must be reviewed annually.

Enforcement

Non-compliance with this policy may result in disciplinary action, including restriction of access, retraining, or termination of employment or contracts. The Security Compliance Team will monitor adherence and escalate unresolved issues to executive management for action.

Version History Table

Version	Date	Description
1.0	05/29/2025	First Draft of Security Maturity Policy

Citations