SNOWBE ONLINE
Policy DEV-02
Security Maturity Policy

Richard Berthelot

DEV-02 - Version # 1.0

March 24 2025

Table of Contents

Purpose

An Enterprise Cybersecurity Maturity Model provides a structure for SnowBe Online to baseline current capabilities in cybersecurity while establishing a foundation for consistent evaluation. By implementing a cybersecurity maturity model, state agencies will not only have a framework for measuring the maturity of their cybersecurity program but also guidance on how to reach the next level as the agency maturity impacts cybersecurity premiums.

Scope

This policy applies to all business units, IT assets, and personnel responsible for cybersecurity within SnowBe Online. It includes all security-related processes, governance structures, risk management strategies, and technical implementations.

Definitions

- **Baseline Security Practices**
  Minimum security controls that must be implemented to ensure fundamental protection of IT systems.
- **Continuous Improvement**
  A process of regularly evaluating and enhancing security practices to adapt to evolving threats and business needs.
- **Maturity Levels**
  A set of defined stages that measure the effectiveness and sophistication of an organization's security capabilities.
- **Patch Management**
  The practice of managing and applying updates to software applications and systems in order to address security vulnerabilities, improve functionality, and maintain system performance.
- **Risk-Based Approach**
  A methodology that prioritizes security improvements based on the likelihood and impact of threats.
- **Risk Management**
  The process of identifying, evaluating, and taking steps to minimize or mitigate risks that could have a negative impact on the organization.
- **Security Maturity Model**
  A structured framework used to assess and improve an organization's cybersecurity posture over time.
- **Vulnerability Management**
  The process of identifying, classifying, remediating, and mitigating security vulnerabilities within a system.

Roles & Responsibilities

Chief Information Security Officer (CISO)
Responsible for overseeing the security maturity program, defining security objectives, and ensuring compliance with industry standards.

IT Security Team
Responsible for conducting security assessments, tracking security maturity progress, and implementing necessary controls to improve security posture.

Compliance Officer
Ensures that security maturity assessments align with regulatory and compliance requirements such as **NIST 800-53 r5**, **PCI DSS**, and **GDPR**.

Risk Management Team
Identifies, evaluates, and mitigates risks associated with SnowBe Online's security posture. Works closely with IT and compliance teams to address security gaps.

Policy

5.1 Maturity Levels

The security maturity of SnowBe Online is evaluated based on the following levels:

Level 1: Initial
Security processes are informal, reactive, and inconsistently applied. Minimal documentation exists, and security controls are implemented ad hoc.

Level 2: Developing
Basic security policies and procedures are in place. Some risk management practices are followed, but enforcement is inconsistent.

Level 3: Defined
Security controls are documented, standardized, and consistently applied across the organization. Risk management practices are established and actively monitored.

Level 4: Managed
Security controls and risk management processes are integrated into business operations. Continuous monitoring and regular security assessments are conducted.

Level 5: Optimized
Security is fully embedded into the organization's culture. Security measures are proactively refined based on real-time threat intelligence and industry best practices.

5.2 Assessment and Evaluation

SnowBe Online will conduct security maturity assessments annually to evaluate its current security posture. These assessments will identify gaps, determine areas for improvement, and establish action plans to enhance security maturity. The assessment process includes:

- Reviewing existing security policies, procedures, and controls.
- Identifying vulnerabilities and weaknesses in the current security framework.

- Measuring progress against defined security maturity levels.
- Developing remediation plans and improvement strategies.

6. Continuous Improvement

Security maturity is an ongoing process that requires continuous monitoring, evaluation, and enhancement. SnowBe Online will:

- Regularly update security policies and procedures to reflect emerging threats and technological advancements.
- Conduct security training and awareness programs for employees to foster a security-conscious culture.
- Leverage security analytics, audits, and threat intelligence to enhance decision-making and risk management.
- Implement automation where possible to streamline security processes and incident response.

Exceptions/Exemptions

Any exceptions to this policy must be documented and approved by the Chief Information Security Officer (CISO). Exceptions may be granted only for business-critical needs where compliance with this policy would significantly hinder operational performance, provided there is an alternative security mitigation in place.

Enforcement

Violations of this Security Maturity Policy will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	March 24, 2025	Daphnie Bruno		Created Security Maturity Policy

Citations

- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- **NIST**: National Institute of Standards and Technology. (n.d.). *NIST Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework
- Georgia Technology Authority's Cybersecurity Capability Maturity Model (SS-20-001)