SNOWBE ONLINE Policy#03
Security Maturity

Your name:Paola Baez Hernandez

< Policy#03 Security Maturity **> -**

Version #03 DATE: 05-29-2025

Table of Contents

Purpose

The purpose of this policy is to create a continuous improvement process that raises SnowBe Online's cybersecurity maturity using established frameworks such as CMMC and the NIST Risk Management Framework.

Scope

This policy applies to all business units, third-party vendors, and internal teams that have access to SnowBe Online systems or sensitive data.

Definitions

CMMC (Cybersecurity Maturity Model Certification): A framework for assessing the maturity of cybersecurity processes.

Risk-Based Prioritization: The process of addressing cybersecurity needs based on potential impact.

Security Maturity: The degree to which an organization's cybersecurity practices are formalized, measured, and continuously improved.

Roles & Responsibilities

- **All Employees:** Participate in required training and process improvements.
- **CISO:** Leads assessments and defines maturity benchmarks and goals.
- **Department Heads:** Ensure team-level practices align with maturity targets.
- **Security Analysts:** Collect and interpret metrics for maturity tracking.

Policy

1. Annual Assessment: Conduct yearly maturity evaluations using CMMC or NIST frameworks.

2. Prioritization: Domains scoring low in maturity must be reviewed and improved first.

3. Training & Documentation: Quarterly training and policy reviews are mandatory.

4. Metrics & Reporting: Maturity level progress will be tracked and presented to executives.

5. Roadmap Development: A 12-month improvement plan must be developed following assessments.

Exceptions/Exemptions

If a domain cannot be improved within the calendar year, a documented exception request must be submitted for CISO approval.

● To ensure compliance with internal standards, exceptions or exemptions requests are handled through a specific procedure. These requests are reviewed, justified, and approved according to SnowBe Online's internal guidelines.

● The dropdown for submitting Exceptions/Exemptions requests can be found on the SnowBe Online associate portal webpage. Allowing staff members to easily request exceptions or exemptions from regular rules and processes, guaranteeing that any deviations are appropriately recorded and examined.

● The request form is available through the “Compliance Forms” tab, located at the top right of the page. This ensures consistency throughout the process; this centralized location makes it simple for employees to find, be able to view, and send requests.

● The form for requesting exceptions or exemptions is titled “Exceptions/Exemptions” within the drop-down window. This clearly labels the form for exception or exemption requests, ensuring that the process is straightforward, and users can identify the correct form to address their specific needs.

● Requests for exceptions or exemptions are made when deviations from standard procedures or policies are necessary due to specific circumstances, such as operational needs, technical constraints, or temporary situations. Any changes are carefully thought through and examined before they are accepted as a result of these requests.

Approval Hierarchy:

● IT: The IT Director or IT Manager will perform the initial review to ensure the requested exemption does not compromise SnowBe Online's security, infrastructure, or compliance.
● Management: Management will review the request to confirm alignment with business objectives and ensure that no critical operations are disrupted.

● Final Authority: The IT Director or IT Manager holds the final authority on all exceptions or exemptions, ensuring decisions align with SnowBe Online’s overall business strategy, security requirements, and compliance obligations.

Approval Notification: Once the request is submitted, the requester will receive an email notification indicating whether the request was approved or denied. The status of the request can also be tracked via the SnowBe Online associate portal webpage.

Enforcement

Failure to meet improvement goals may trigger additional oversight or reassignment of responsibilities. Non-compliance may be escalated to executive leadership.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
V.03	05-29-2025	Paola Baez		Initial Security Maturity policy established

Citations

https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

https://www.neosystemscorp.com/cmmc-compliance-services/cmmc-101/what-is-the-cmmc-certification-process/?creative=690759188564&keyword=cmmc readiness&matchtype=p&network=g&device=c&utm_source=google&utm_medium=ppc&utm_campaign=CMMC-MOFU - Search&utm_term=cmmc readiness&gad_source=1&gad_campaignid=21018200849&gbraid=0AAAAAD8_cE_MjTouNaHUW06I83ucIHTWb&gclid=Cj0KCQjw9O_BBhCUARIsAHQMjS7mpPmYfvmVtKg-yOSOrBpFO9AH_4jRsxH1y5ijTqA7jnAgKcMI6zgaAnhGEALw_wcB