SNOWBE ONLINE

CMMC1 – Security Maturity Policy

Your name: Davon Richardson

Version #1

DATE: 09-25-2025

<CCM1> – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Davon Richardson
DATE: 05-26-2025

Table of Contents

Purpose

The purpose of this Cybersecurity Maturity Model provides a structure for SnowBe to baseline current capabilities in cybersecurity while establishing a foundation for consistent evaluation. By implementing a cybersecurity maturity model, SnowBe will not only have a framework for measuring the maturity of their cybersecurity program, but also a guide on how to reach the next level as the company maturity impacts cybersecurity premiums.

Scope

This policy applies to all members of SnowBe, including employees and management involved in developing systems and software.

Definitions

None

Roles & Responsibilities

Executive leadership – ensures compliance aligns with SnowBe goals

IT and Cybersecurity team – implements technical safeguards, maintain the system and information integrity.

Policy

The SnowBe Cybersecurity Capability Maturity Model is a tool that the company shall use to develop, assess and refine the company's Cybersecurity Program. The maturity model will be used annually to evaluate, rate and score each team's maturity level as it relates to the Center for Internet Security (CIS) 20 Critical Security Controls. SnowBe's Cyber Risk Scores will be determined by the company's Cybersecurity questionnaire which shall be annually completed by each team.

MATURITY LEVEL DETAILS

A maturity level is a well-defined evolutionary plateau toward achieving a mature cyber capability process. Each maturity level provides a layer in the foundation for continuous process improvement.

Maturity levels consist of a predefined set of process areas. The maturity levels are measured by the achievement of the specific and generic goals (CIS 20 Critical Controls) that apply to each predefined set of process areas. The following sections describe the characteristics of each maturity level in detail.

Maturity Level 1 (Initial): Processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes.

Maturity Level 2 (Repeatable): At maturity level 2, an organization has achieved all the specific and generic goals of the maturity level 2 process areas. In other words, the projects of the organization have ensured that requirements are managed and that processes are planned, performed, measured, and controlled.

Maturity Level 3 (Defined): At maturity level 3, an organization has achieved all the specific and generic goals of the process areas assigned to maturity levels 2 and 3. At maturity level 3, processes are well characterized and understood, and are described in standards, procedures, tools, and methods.

Maturity Level 4 (Quantitatively Managed): At maturity level 4, an organization has achieved all the specific goals of the process areas assigned to maturity levels 2, 3, and 4 and the generic goals assigned to maturity levels 2 and 3.

Maturity Level 5 (Optimizing): At maturity level 5, an organization has achieved all the specific goals of the process areas assigned to maturity levels 2, 3, 4, and 5 and the generic goals assigned to maturity levels 2 and 3.

Exceptions/Exemptions

Anyone will initiate an exception request by contacting the IT department for Request an Exception to a Security Policy, Standard, or Procedure item, which can guide users through the policy exception request process as follows:

1. Once the form is submitted, the request is assigned to the IT Compliance team to review.
2. An IT Compliance team member works with the user to
    - assess the risks created by the exception,
    - evaluate potential alternatives,
    - provide recommendations, and
    - determine the appropriate departmental and if applicable, the data steward's approval(s), the user needs to obtain,
3. Once the appropriate approvals are obtained, the IT Compliance team member will reply via email with documented approval or denial of the request (along with request details) to the requestor and/or user for whom the exception was requested, copying the department head/chair and vice president/dean approvers, as well as company Audit.
4. If the exception is granted and approval is obtained, the IT Compliance member will provide

the user with any additional assistance as needed, such as coordinating with the relevant data steward(s) or other individual(s) who have a role in fulfilling the exception request.

5. If the exception is not granted, SnowBe Online Information Security will work with the user to define a reasonable deadline for compliance.

6. If the exception is not granted, the user may appeal the decision to the Chief Information Officer (CIO)

7. The user will be notified prior to expiration that the exception duration is ending. The user must then submit a new exception request or notify InfoSec that the exception is no longer needed.

Enforcement

Violations of any SnowBe Online policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of these policies may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
V1	May 10, 2025	Group 4	Davon Richardson	Exceptions/Exemptions & Enforcement
V2	September 25, 2025	Davon Richardson	Davon Richardson	Purpose/Scope/Roles and responsibilities/Policy

Citations

University Of Virginia
Exemptions
https://security.virginia.edu/exceptions

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

Georgia Government
Purpose
Scope
Roles and responsibilities
Policy
https://gta-psg.georgia.gov/psg/cybersecurity-capability-maturity-model-ss-20-001