ITP111 Security Maturity Model Policy V 1.0

Status: ⊡ Working ☐ Draft ☐ Approved ☐ Adopted

Document owner: Ian Corbitt - SnowBe

4/28/2023

ITP111 Security Maturity Model Policy

Purpose

An Enterprise Cybersecurity Maturity Model provides SnowBe a baseline for their 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 guidance on how to reach the next level.

Scope

SnowBe employees and other covered individuals (e.g., SnowBe affiliates, vendors, independent contractors, etc.) that perform any type of software or systems development work under the auspices of SnowBe.

Definitions

SnowBe utilizes various industries' standard definitions compiled and managed SnowBe Information Technology for all information security and privacy. Refer to SnowBe IT Document ITD-002, Technical Definitions.

Roles and Responsibilities

Functional Officer - Chief Information Security Officer: Overall owner of SnowBe's IT Security subdivision and all its assets. Tasked with ensuring all IT assets are secured in accordance with this and all applicable laws, regulations, and business policies.

Responsible Officer - Chief Information Officer: Overall owner of SnowBe's IT division and all its assets.

Policy

The SnowBe Cybersecurity Capability Maturity Model is a tool that SnowBe shall use to develop, assess and refine the Cybersecurity Program. The maturity model will be used annually to evaluate, rate and score SnowBe's maturity level as it relates to the Center for Internet Security (CIS) 20 Critical Security Controls. Cyber Risk Scores will be determined by SnowBe's technology status questionnaire which shall be completed annually. This approach allows for the prioritization and consideration of control effectiveness as demonstrated by the CIS Controls, in business and IT areas across SnowBe.

Maturity Levels:

- 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.

- Cyber Risk Tiers: Cyber Risk Tiers are risk scores based on SnowBe's maturity. The scores ranging from 1.0 - 5.0 are an indication of SnowBe's Cyber Risk.

ITP111 Security Maturity Model Policy V 1.0

Status: ⊡ Working ☐ Draft ☐ Approved ☐ Adopted

Document owner: Ian Corbitt - SnowBe

4/28/2023

Maturity Levels	Cyber Risk Tiers
Level V- CIS Controls 1-20 (Optimized)	Risk Score: 1.0
Level IV- CIS Controls 1-19 (Managed)	Risk Score: 1.5
Level III- CIS Controls 1-19 (Defined)	Risk Score: 2.0
Level II- CIS Controls 1-6, 10, 17 (Repeatable)	Risk Score: 3.0
Level I- CIS Controls 1-6, 10, 17 (Initial/Informal)	Risk Score: 4.0
Level 0- No processes	Risk Score: 5.0

Exceptions/Exemptions

Exceptions or exemptions for this policy to this policy are reviewed and enacted on a case-by-case basis. For further details on obtaining an exception or exemption from this policy, please refer to SnowBe IT Policy ITP-042, IT Policy Exceptions and Exemptions.

Enforcement

This policy is self-enforcing by the authority granted to it by all local and federal laws as well as SnowBe business operations policies and SnowBe IT Policy ITP100. This policy must be adhered to except in the exceptions and exemptions noted above or in SnowBe Document ITD-001 IT Exceptions and Exemptions, otherwise one or more of the following actions may result:

- Written warning regarding policy violation.
- Disciplinary action, up to and including termination.
- Legal action taken against the individual(s) outside of compliance.

Version History

Version	*Date*	*Owner*	*Approved*	*Description*
1.0	*4/28/2023*	*Ian Corbitt*	*Ford Prefect*	*Initial Release*

Citations

State of Georgia: https://url.vogon.dev/DarkTrustyAppointment