SNOWBE ONLINE Policy#

Maturity Model

Your name: Eddy Cruz Pena, Travis Ferrufino, Vanessa Campbell, Jeremey Sarduy, David Perez Puello

<Maturity Model> - Version # 1.0

DATE: 07/27/24

Table of Contents

Purpose

This is an Enterprise Cybersecurity Maturity Model which 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, SnowBe will not only have a framework for measuring the maturity of their cybersecurity program, but also a guidance on how to reach the next level as SnowBe's maturity grows and continues to change.

Scope

This policy covers all entities who work for SnowBe Online, including all employees, contractors, and third-party service providers who have access to SnowBe Sensitive data and Systems. This Policy covers all aspects of cyber security, such as risk assessment, incident response, data protection, along with ensuring SnowBe security is compliant with the Center for Internet Security's (CIS) Top 20 Critical Security Controls. The policy addresses all aspects of SnowBe Onlines's IT infrastructure, equipment and data resources, which will ensure consistency and a comprehensive approach to improve Cyber Security practices across SnowBe Online's landscape.

Definitions

Chief Information Officer (CIO): The executive responsible for managing and overseeing the information technology and security strategy of the organization.

Critical Security Controls: A set of prioritized cybersecurity best practices, guidelines, and recommendations provided by the Center for Internet Security (CIS) to help organizations improve their cybersecurity defenses.

Cybersecurity Maturity Model: A framework that provides a structured approach to assessing and improving the cybersecurity capabilities and processes of an organization.

Incident Response: The process of identifying, managing, and mitigating the effects of a cybersecurity incident, including breach containment and recovery efforts.

Risk Assessment: The systematic process of identifying, evaluating, and prioritizing potential risks to an organization's information systems and data.

Security Policies: Officially documented rules and guidelines that govern the security measures and practices within an organization.

Third-Party Service Providers: External organizations or individuals contracted to provide services to SnowBe Online, who may have access to the company's information systems or data.

Vulnerability Management: The process of identifying, assessing, and mitigating security vulnerabilities in an organization's information systems and software.

Roles & Responsibilities

Chief Information Officer (CIO):

- Oversee the development, implementation, and enforcement of cybersecurity policies and practices.
- Approve and review any exceptions or exemptions to security policies.
- Lead the organization's cybersecurity strategy and risk management efforts.

Information Security Team:

- Implement and maintain the cybersecurity measures outlined in the organization's policies.
- Conduct regular risk assessments and vulnerability management activities.
- Respond to and manage cybersecurity incidents.

Department Heads:

- Ensure that their respective departments comply with the organization's cybersecurity policies and procedures.
- Report any cybersecurity incidents or concerns to the Information Security Team.

Employees and Contractors:

- Adhere to the organization's cybersecurity policies and procedures.
- Participate in required cybersecurity training and awareness programs.
- Report any suspicious activities or potential security incidents to the Information Security Team.

Third-Party Service Providers:

- Comply with SnowBe Online's cybersecurity requirements and standards.
- Cooperate with the Information Security Team to ensure the protection of data and systems.

Data Protection Officer (DPO):

- Oversee the organization's data protection strategy and ensure compliance with relevant data protection laws and regulations.
- Advise on data protection impact assessments and handle data protection-related inquiries and incidents.

Audit and Compliance Team:

- Conduct regular audits of the organization's cybersecurity practices ensuring compliance with internal policies and external regulations.
- Report findings and recommend improvements to the CIO and Information Security Team.

Training and Awareness Coordinator:

- Develop and deliver cybersecurity training programs for employees and contractors.
- Promote awareness of cybersecurity best practices and policies throughout the organization.

Policy

SnowBe Online's Cybersecurity Capability Maturity Model is a tool that SnowBe shall use to develop, assess and refine its current 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. This approach allows for the prioritization and consideration of control effectiveness as demonstrated by the CIS Controls, in business and IT areas across the State.

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 depend 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

Employees or partners seeking an exemption from any of SnowBe Online's security policies are required to submit a written request addressed to the Chief Information Officer (CIO). This request must clearly outline the reasons for the exemption, the specific policy or policies involved, and any proposed measures to mitigate potential risks during the exemption period. The aim is to ensure that each request is thoroughly documented, establishing a formal paper trail for accountability and review.

For instance, if a store manager identifies that older point of sale (POS) systems in certain storefronts cannot support the latest encryption standards due to hardware limitations, a written exemption request would detail these limitations, the store's current security measures, and any temporary solutions proposed until the systems can be updated.

Upon receipt, each request will be evaluated based on its merit, the potential impact on SnowBe Online's security posture, and the feasibility of the proposed mitigating measures. The CIO, in consultation with relevant security and data protection officers, will make the final decision on granting the exemption.

If the request is approved, the requester will be granted the exemption for a period of one year starting from the date of approval. This time-bound approach ensures that exemptions are temporary and subject to reevaluation, maintaining the flexibility to adapt to evolving security needs and technological advancements. Should the security plan undergo significant alterations or updates, all granted exemptions will be reviewed, and requesters may be required to submit new applications for approval, ensuring continuous alignment with SnowBe Online's security objectives and compliance requirements.

If an exemption request is initially denied, the requester must wait 3 months before reapplying. Subsequent requests can be submitted for review after the waiting period, provided they include additional reasons and justification for the exemption requested.

This process underscores the importance of rigorous documentation and periodic review in managing exceptions to security policies, ensuring that SnowBe Online maintains a robust and adaptable security framework even as it navigates the challenges of evolving technology and business practices.

Enforcement

All individuals who work for SnowBe Online directly or who are contractually obligated, such as third-party vendors, are required to comply with federal and state laws, SnowBe policies, and procedures pertaining to the security, integrity, and availability of sensitive data. Any employee or contractually obligated persons who have access to SnowBe data and engage in unauthorized use, disclosure, alteration, or destruction of data is in violation of this plan and will be subject to appropriate disciplinary action, including but not limited to suspension, termination and or legal action taken against those responsible.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	07/27/24	SnowBe Online		Initial Draft of Security Maturity Policy

Citations

Georgia Technology Authority. (2019, October 1). Cybersecurity Capability Maturity Model (SS-20-001). Georgia.gov. Retrieved July 27, 2024, from https://gta-psg.georgia.gov/psg/cybersecurity-capability-maturity-model-ss-20-001