SNOWBE SECURITY PLAN

Version Number 5.0

02/25/2023

Table of Contents

1. Introduction

Security is a critical aspect of modern technology and essential to protecting sensitive information and systems. A security plan systematically safeguards sensitive information, IT resources, and an organization's critical infrastructure. This security plan aims to outline the measures and procedures that will be taken to secure the organization's IT systems, networks, and data and to ensure the confidentiality, integrity, and availability of information.

The security plan will guide managing risk, protecting against threats, and ensuring the continuity of operations. It will also outline the responsibilities of various stakeholders, including employees, contractors, and third-party service providers, in maintaining the organization's IT systems and data security. The security plan will be regularly reviewed and updated to reflect changes in the threat environment and to ensure its ongoing effectiveness in protecting the organization's critical information and assets.

2. Scope

This security plan covers the information technology (IT) systems, networks, and data of SnowBe Online. This includes all desktops, laptops, servers, mobile devices, and cloud services used by employees, contractors, and third-party service providers.

This security plan will cover the following types of data:

- Personal information, such as names, addresses, and social security numbers
- Financial data, such as credit card numbers and bank account information
- Intellectual property, such as trade secrets and confidential business information

3. Definitions

Access Privileges:

- The rights granted to a user or group of users to perform certain actions, such as reading, writing, executing, or modifying data or resources within a computer system or network.

***Account*:**

- Any combination of a User ID (sometimes called a username) and a password grants an authorized user access to a computer, an application, the network, or other information or technology resources.

Account Manager:

- A professional responsible for managing the relationships between an organization and its clients, customers, or other stakeholders regarding cyber security solutions and services.

Authentication Mechanism:

- A mechanism that verifies user identities to ensure authorized persons can access the resources they need and to keep unauthorized persons from gaining access to resources.

CMMC:

- The Cybersecurity Maturity Model Certification is a unified cybersecurity standard developed to enhance the protection of CUI across the Defense Industrial Base (DIB).

CUI:

- Controlled Unclassified Information requires safeguarding under applicable laws, regulations, and government-wide policies.

Cryptographic Mechanisms (Cryptographic Modules):

- Any hardware, firmware, or software combination implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques, and random-number generation.

Data Integrity:

- Maintaining data accuracy, consistency, and reliability throughout its entire lifecycle. It ensures the data remains unaltered and free from unauthorized modification, deletion, or corruption.

Highly restricted data:

- An organization's most sensitive and confidential information requires the highest level of protection.

Impact:

- The extent of the damages resulting from an adverse event (i.e., realized threat) affecting Company Information Resources.

Information Assets:

- Any data, knowledge, or intellectual property that has value for an organization. This can include sensitive information such as customer data, trade secrets, financial records, confidential business plans, and non-sensitive information such as product or marketing materials.

Information assets can take many forms, including databases, documents, emails, images, and audio and video files.

***Information Resource*:**

- An asset that is essential to an organization's business. Including hardware assets (e.g., workstation, server, laptop), digital form (e.g., data files stored on electronic or optical media), material form (e.g., on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means, including courier, electronic, or verbal communication.

Patch:

- A software update designed to fix or improve a program. This includes fixing security vulnerabilities and other bugs and improving usability or performance.

Patch Management:

- Identifying, acquiring, installing, and verifying software applications and systems patches.

Password:

- A secret combination of characters is used to authenticate a user's identity.

Password Manager:

- A software tool used to store and manage passwords securely.

PCI DSS:

- Payment Card Industry Data Security Standard

Privilege

- The special rights, permissions, and access granted to a user, program, or process within a computer system or network. These privileges determine the user's actions and resources they can access.

Restricted Data:

- Any sensitive information is considered highly confidential and protected by specific legal or regulatory requirements.

SDLC:

- The conceptualizing, designing, developing, testing, deploying, and maintaining information systems and applications.

Security Maturity:

- The effectiveness of an organization's cybersecurity practices, the ability to respond to threats, and the continuous adaptation and improvement of security controls.

Stakeholders:

- All individuals or groups that participate in or are affected by SDLC activities.

4. Roles & Responsibilities

Chief Information Security Officer (CISO):

- Responsible for the organization's information systems' overall security strategy and implementation.

Compliance Officer:

- Ensures that the organization complies with applicable security regulations and standards.

Database Administrator (DBA):

- Maintain the organization's databases' security and ensure user accounts are assigned the minimum privileges necessary to access the data.

Information Security Officer (ISO):

- Responsible for ensuring the organization's information systems and data security.

Information System Owner:

- The Information System Owner (SO) is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

IT Department:

- The IT Department must provide training and awareness programs to all employees to ensure they understand the importance of security and their role in protecting SnowBe's assets.

- The IT Department must monitor the network for security incidents, investigate and resolve any incidents, and report them to management.

- The IT Department must maintain up-to-date records of all security incidents and implement remediation measures to prevent similar incidents.

IT Security Team:

- Responsible for the implementation and management of security controls.

Network Administration Team:

- Responsible for managing and maintaining the organization's network infrastructure.

Security Operations Center (SOC):

- Responsible for monitoring and responding to security incidents and implementing security controls.

SnowBe Online Employees:

- All employees must understand and comply with SnowBe's security policies and procedures.
- Employees must report any security incidents or concerns to the IT Department immediately.
- Employees must attend security training and awareness programs the IT Department provides to ensure they remain up-to-date with security best practices.

Systems Administrator:

- Installs, configures, and maintains the organization's systems, including those that enforce the least privilege.

Third Parties:

- Third-party service providers are responsible for assuring those systems, system components, and services they provide are secure and do not negatively impact the security of pre-existing systems by implementing secure information systems and communications protection practices.

5. Statement of Policies, Standards, and Procedures

5.1 Policies

SP-1 Identity and Access Management

- Identity and access management ensures the accurate identification of authorized SnowBe staff and provides secure, authenticated access to network-based services. This system is based on a set of principles and control objectives, including:
  - Unique identification and assignment of access privileges to SnowBe staff
  - Limiting access to information resources to authorized individuals only
  - Regular review of staff membership and access rights
  - Maintenance of effective access mechanisms through changes in technology.
- Access control refers to controlling access to systems, networks, and information based on SnowBe's business and security needs. The objective is to prevent unauthorized access to SnowBe's valuable information assets. Access control measures include secure identification, authentication, and authorization methods.

AC-2 Account Management

- SnowBe Online implements a comprehensive account management system to secure information systems. This includes identifying and selecting different types of accounts, assigning account managers, specifying authorized users and privileges, requiring approval for account creation, monitoring account use, disabling inactive or temporary accounts, and automating the account management process. The system also automatically audits account actions and notifies IT personnel. The accounts are reviewed for compliance bi-yearly, and a process is established for reissuing shared/group account credentials when individuals are removed from the group.

AC-6 Least Privilege

- The least privilege and authorized access control principle is crucial to secure sensitive information. The information system should allow only necessary authorized access for users and limit direct access to hardware and software. Users should use non-privileged accounts for non-security functions. The system should audit the execution of privileged functions and prevent non-privileged users from executing them, including disabling security measures.

SC-28 Protection of Information at Rest

- outlines the security measures to protect restricted or highly restricted data at rest. Cryptographic mechanisms must be implemented to prevent unauthorized disclosure and modification of such data. All restricted or highly restricted data on non-volatile storage devices must be encrypted with FIPS 140-2 compliant encryption. Additionally, recording data onto write-once media and storing data on physically separate non-mobile storage devices with cryptographic protections are recommended. This policy is optional for low-risk information systems.

SC-8 Transmission Confidentiality and Integrity

- outlines several security measures to protect a company's network and data. It includes using network monitoring tools to detect suspicious traffic, securing interfaces between the company and non-company networks, implementing standardized authentication mechanisms for users and devices, and using secure protocols for network management. The policy also requires a risk management determination for each type of confidential information and the use of current secure-transport protocols for data transfer. Finally, the policy includes monitoring for anomalies or known signatures through intrusion detection and prevention systems and network behavior analysis tools.

SP-2 PCI DSS Compliance

- PCI DSS is a set of security controls designed to ensure that organizations handling credit card information maintain a secure environment for protecting this sensitive data. The key aspects of the PCI DSS include building and maintaining a secure network, protecting cardholder data, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy. These controls aim to prevent unauthorized access to cardholder data, protect the confidentiality and integrity of this data, and maintain compliance with industry standards and regulations.

SP-3 Change Management

– outlines the requirements for managing changes to SnowBe Online Information Resources. Changes must be documented and classified based on importance, urgency, impact, and complexity. Change documentation must include specific details such as date, owner and custodian contact information, nature of the change, and change classification. Significant changes must be scheduled and communicated to SnowBe Online Information Resource owners. Change control documentation must be maintained and the relevant authority must approve changes. Emergency changes may be implemented immediately and then documented retrospectively.

SP-4 Physical Security

– Physical security measures, such as controlling physical access to equipment and data, minimize unauthorized access, damage, and interference with information and information systems on the SnowBe Online network. These measures ensure the protection of information technology assets and provide a secure environment.

SP-5 System Development Life Cycle

– The System Development Life Cycle (SDLC) Policy at SnowBe provides a structured framework for developing and implementing systems, ensuring efficiency, thorough documentation, and rigorous testing at every stage. The policy delineates nine phases - Analysis, Planning, Design, Development, Testing, Deployment, Maintenance, Evaluation, and Disposal, with continual emphasis on security considerations throughout each phase. This policy ensures systematic, secure, and efficient system development, with strict enforcement measures for compliance.

SP-6 Software Patch Management

– The Software Patch Management Policy at SnowBe outlines a structured approach to managing system updates and vulnerabilities. It encompasses timely identification, testing, approval, and deployment of patches to maintain system security and functionality. The policy also outlines roles, responsibilities, and the mandatory nature of updates, ensuring regular monitoring and enforcement for non-compliance.

SP-7 Security Maturity

– SnowBe's Security Maturity Policy provides a framework for continuously enhancing cybersecurity practices, focusing on identifying, managing, and reducing security risks. The policy emphasizes adopting systematic, repeatable, and measurable security procedures, underlining the organization's commitment to aligning with industry best practices, compliance requirements, and regulatory standards for information security.

5.2 Standards and Procedures

5.2.1 Standards

SBS-1 Password Standard

- Establishes requirements for creating and maintaining strong and secure passwords to protect the confidentiality, integrity, and availability of SnowBe Online's information resources. The standard requires all employees to use strong passwords, change them periodically, and not reuse them for multiple accounts. It also prohibits the use of easily guessable information, recommends the use of a password manager, and mandates the use of multi-factor authentication wherever possible.

5.2.2 Procedures

SBP-1 Creating a New Account

- This procedure outlines the steps for SnowBe employees to create their accounts. It explains the purpose and scope of the procedure, including who is responsible for creating accounts and the necessary materials needed for the task. The procedure also outlines the steps for employees to follow, including accessing the account creation portal, entering their personal information and contact details, selecting a secure password, and accepting the terms and conditions.

SBP-2 Creating a Password

- It involves selecting a strong password that meets specific criteria, changing the password every 90 days, and ensuring that it is not easily guessable, written down, or shared with anyone. The procedure also recommends using a password manager and manual entry of passwords.

6. Exceptions/Exemptions

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should expressly state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions, and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

7. Version History

Version	Change Date	Description
1.0.	02/06/2023	The first draft of the security plan. Adds the first three policies and updates definitions and roles.
2.0.	02/13/2023	Adds two policies and updates introduction, scope, definitions, roles, and exceptions accordingly.
3.0	02/19/2023	Adds three policies and one procedure and updates definitions and roles.
4.0	02/25/2023	Added Statement of Policies, Standards, and Procedures header, Standards and Procedures sub-headers, Password Standard, Creating a Password procedure, and relevant definitions and roles and responsibilities. Updated Policies and Standards and Procedures headers (now sub-headers) and policy, standard, and procedure names and numbering.
5.0	06/24/2023	Adds three polices