SNOWBE ONLINE SECURITY PLAN

Davon Richardson – section 2

Table of Contents

Section 1: Introduction

This Information Security Plan outlines SnowBe Online ongoing efforts to secure information related to stakeholders who provide sensitive information to the company to implement safeguards to protect non-public personal data, information and resources. These safeguards are provided to:

- Make reasonable efforts to ensure the security and confidentiality of sensitive data, information and resources
- Protect against anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of confidential data, information and resources that could result in substantial harm or inconvenience to any consumer.

SnowBe Online adopted the following Information Security Plan as a measure to protect the confidentiality, integrity and availability of the brand's as well as any Information Technology (IT) assets. This plan provides for mechanisms to:

- Identify and assess the risks that may threaten sensitive data, information and resources maintained by the company
- Manage and control these risks
- Implement and review the plan
- Adjust the plan to reflect changes in technology, the sensitivity of confidential data, information and resources, and internal or external threats to Information Security.

Section 2: Scope

This plan applies to the entire SnowBe Online Company and its network, including the President, Vice Presidents, and Department Heads, staff, temporary employees, and third parties who have access to SnowBe Online information technology resources. Such assets include data, images, text, or software, stored on hardware, paper or other storage media.

Section 3: Definitions

N/A

Section 4: Roles - Responsibility

Executive Management: Will establish the overall approach to governance and control by forming the Information Security Board of Review (ISBR) to provide strategic direction, ensure objectives are achieved, ascertain risks are managed appropriately, and verify that the company's resources are used responsibly.

IT governance is the responsibility of Executive Management and consists of leadership, organizational structures, and processes to ensure that the company's information technology sustains and extends SnowBe Online's strategies and objectives.

The Office of Information Technology (OIT) shows its commitment to developing and implementing good internal controls as well as ensuring the promotion and awareness of IT requirements and plans throughout the company. SnowBe Online’s strategic vision is linked with the IT department’s goals and objectives, ultimately assuring that the Company meets customer and legal requirements while undergoing continual improvement.

Section 5: Statement of Policies, Standards and Procedures

Policies

PC1: PCI Compliance

The PCI DSS is a mandated set of requirements agreed upon by the major credit card companies. The security requirements apply to all transactions surrounding the payment card industry and the merchants or organizations that accept these cards as a form of payment.
SnowBe must comply with the PCI DSS to accept card payments and avoid penalties. This policy and additional supporting policies:

- Provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions
- Reduce the institutional risk associated with the administration of payment cards
- Promote proper internal control
- Promote compliance with the PCI DSS

Policy 1: Access Control Policy:

The Access Control Policy determines the settings used for limiting access to university computer systems and information stored on those systems. The controls listed provide guidance on account management and privilege assignments. The guidance defines the assignment of roles and associated business functions. Other controls include login time, screen saver requirements, and similar activity-based controls. This policy establishes a minimum expectation, with respect to access controls, in order to protect data stored on computer systems at SnowBe.

Policy 3: Physical Security Policy:

The purpose of this policy is to protect the company's physical information systems by setting standards for secure operations.

Policy 5: Network Security Policy:

SnowBe Online seeks to maintain confidentiality, integrity, and availability of information about its employees and customers, as well as its general affairs. It is extremely important to the Company to preserve its reputation and its integral parts.

Security of the Company’s networks and associated systems is an important part of this aim, and this policy sets out the ways in which the Company will seek to secure its networks.

Policy 7: Software Management Policy:

This Software Management policy is a sub-policy of the Information Security policy (ISP-01) and sets out the principles and expectations for the security aspects of managing software

Policy 9: Acceptable Use Policy:

The purpose of this policy is to outline the acceptable use of computer equipment at SnowBe Online. These rules are in place to protect the employees and SnowBe Online consumers. Inappropriate use exposes SnowBe Online to risk including virus attacks, compromises of the network systems and services, and legal issues.

Policy 10: Password Policy:

The purpose of this policy is to specify guidelines for the use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

Policy 14: Firewall Policy:

This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to SnowBe Online's network and information systems.

Policy 15: Remote Access Policy:

This policy defines standards for staff to connect to the SnowBe Online network from a remote location. These standards are designed to minimize potential exposures including loss of sensitive information, and limit exposure to security concerns through a consistent and standardized access method.

AC-1 Access Control:

This policy covers all SnowBe Online information and systems used, managed, or operated by a contractor, agency, or other organization on behalf of SnowBe Online. This policy applies to all SnowBe Online employees, contractors, and all other users of SnowBe Online information and systems supporting the operation and assets of SnowBe Online. All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of SnowBe Online data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Access Control security controls.

AC-2: Account Management:

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to SnowBe Online information resources. An account, at minimum, consists of a user ID and a password. Supplying account information will usually grant access to some set of services and resources. This policy establishes guidelines for issuing and managing accounts.

AC-3: Access Enforcement:

Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

AC-7: Unsuccessful Logon Attempts:

The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically released after a predetermined, organization-defined time-period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

AC-8: System Use Notification and AC-9 Previous Logon Notification:

System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content. Previous logon notification is applicable to system access via human user interfaces and access to systems that occur in other types of architectures. Information about the last successful logon allows the user to recognize if the date and time provided is not consistent with the user’s last access.

AC-17: Remote Access:

The purpose of this policy is to define the rules and requirements for connecting to our organization’s network from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

AC-18: Wireless Access:

The purpose of this policy is to state the standards for wireless access to the company's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

AC- 19 Access Control for Mobile Devices:

The purpose of this policy is to establish the procedures and protocols for the use of mobile devices and their connection to the network.

CCM1 – Change Control Management Policy:

The purpose of this policy is to ensure that all changes to SnowBe IT Resources minimize any potential negative impact on services and Users.

SDLC1 – System Development Lifecycle

The purpose of an SDLC methodology is to provide IT Project Managers with tools to help ensure successful implementation of systems that satisfy SnowBe’s strategic and business objectives. The documentation provides a mechanism to ensure that executive leadership, functional managers and users sign off on the requirements and implementation of the system. The process provides SnowBe Project Managers with the visibility of design, development, and implementation status needed to ensure delivery on time and within budget.

PM1 – Patch Management Policy

The purpose of this patch management policy is to achieve the following objectives: Mitigate security risks (Address vulnerabilities and reduce the risk of security breaches, data loss, and unauthorized access.) Ensure system stability (Minimize operational disruptions and system failures). Maintain compliance and accountability (Emphasize our commitment to responsible IT management and compliance with relevant laws, regulations, and industry standards.) Enhance user trust (Foster trust among users, clients, and partners who rely on the security and reliability of our systems.)

CMMC1 – Security Maturity Policy

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.

Standards and Procedures

NACP 1: New Account Creation Procedure

The purpose of this procedure is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to IT resources.

Computer accounts are the means used to grant access to SnowBe's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for SnowBe usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

NPP 1: New Password Procedure

The purpose of this procedure is to detail step by step instructions on how to create a password for a SnowBe Account.

PWS 1: Password Standard

The purpose of this standard is to specify guidelines for the use of passwords. Most importantly, this standard will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this standard will educate users on the secure use of passwords.

Section 6: 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.

Section 7: Version History Table

Version	**Date**	**Description**
Version 1	05-08-2025	Exception/Exemptions
Version 2	05-12-2025	Policies
Version 2.1	05-15-2025	Access Controls Policies
Version 3	05-26-2025	Policies/standards and procedures
Version 4	05-29-2025	Standard and Procedures
Version 5	09-25-2025	Policies

Citations

Howard University
Introduction

https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf

Michigan Technical University
Scope
Roles & Responsibilities
https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

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