SNOWBE ONLINE SECURITY PLAN

Group Member Names: Group 2
James Ingram
John Bays
Jose Rosario
Thomas Trippe

Version # 1.0
Date: 03/30/2025

Table of Contents

Section 1: Introduction

The purpose of this plan is to ensure the confidentiality, integrity, and availability of data, define, develop, and document the information policies and procedures that support the SnowBe Online goals and objectives, and allow the SnowBe to satisfy its legal and ethical responsibilities regarding its IT resources. Information security policies and procedures represent the foundation for the SnowBe Online ISP. Information security policies serve as overarching guidelines for using, managing, and implementing information security throughout SnowBe Online Tech. Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud, and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in business operations. When consistently applied throughout SnowBe Online, these policies and procedures ensure that information technology resources are protected from various threats to ensure business continuity and maximize the return on investments of business interests. This plan reflects SnowBe Tech's commitment to stewardship of sensitive personal information and critical business information in acknowledgment of the many threats to information security and the importance of protecting the privacy of SnowBe constituents, safeguarding vital business information, and fulfilling legal obligations. This plan will be reviewed and updated at least once a year or when the environment changes. This plan provides mechanisms to identify and assess risks, manage and control those risks, and implement and review the plan to maintain compliance with legal and institutional requirements. The intent is to ensure business continuity while minimizing risk to sensitive information and IT assets.

Section 2: Scope

The plan applies to the entire SnowBe Online organization, including its personnel, IT assets, infrastructure, data, and third-party services.

This includes:

- All data stored, processed, or transmitted by SnowBe Online.
- IT assets and infrastructure owned, leased, or managed by SnowBe Online, including hardware, software, and network systems.
- Third-party services that access, process, or manage SnowBe Online data.

Section 3: Definitions

Access Control: refers to the process of controlling access to systems, networks, and information based on business and security requirements.

Availability: Ensuring timely and reliable access to and use of information…" A loss of availability is the disruption of access to or use of information or an information system.

Baseline Security: Fundamental security measures that must be in place to protect systems.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Continuous Monitoring: Ongoing assessment of security controls and threats.

Data Custodian: Implements technical and physical safeguards, documents procedures, and provisions or de-provisions access to institutional data.

Data Steward: An employee responsible for the lifecycle and protection of institutional data.
Integrity: Guarding against improper information modification or destruction and ensuring nonrepudiation and authenticity.

Installation and Validation: A system reboot is required to successfully install most security patches. Until the reboot occurs, the computer remains vulnerable to attacks which the installed patch protects against. IS understands the impact an ill-timed reboot can have on user productivity. In order to provide the SnowBe community with as much flexibility as possible, security updates will be deployed using an “optional-mandatory” method. The optional-mandatory method will allow users to install scheduled update at their convenience before a deadline occurs. Users will be provided five (5) business days to select the installation time of their choosing for deployed patches. After the deadline passes, updates will automatically install and may enforce reboots of the computer as the updates require. It is strongly recommended that users install the updates as soon as possible to ensure that end points are protected and rebooting does not disrupt work. When updates are available, a notification will appear in the system tray. The message will continue to appear daily until the updates are installed and will appear more frequently as the deadline approaches

Mandatory Reboot Exemption: There is the possibility of academic or administrative processes being negatively impacted even with a five-day window for users to apply patches. Users who could be impacted in this scenario may contact the SnowBe Helpdesk and request to be temporarily exempted from the mandatory reboot process. The endpoints being exempted will still have patches deployed regularly, but it will be the responsibility of the end user to reboot the machine to apply those security patches. Each request will be reviewed on a case by case basis and will have a limited duration for exemption.

Out of Band Updates: On occasion a software vendor will release a highly critical security patch outside of their normal release cycle. The usual reason for the release of an out-of-band patch is the appearance of an unexpected, widespread, destructive exploit that will likely affect a large number of users. In the event of a published out of band patch, Information Services (IS) will expedite the validation process. Once validated, users will have two (2) business day to install and reboot their machine to apply the patch. After the deadline passes, updates will automatically install and may enforce reboots of your computer as the updates require. IS will communicate to the campus via Pilots announcements in the event of an out of band update deployment.
Private Data: Data whose unauthorized disclosure could cause moderate harm.

Restricted Data: Data whose unauthorized disclosure could cause significant harm to the organization.

Risk Assessment: The process of identifying, evaluating, and prioritizing risks associated with potential threats to system security.

Risk-Based Approach: Prioritization of security measures based on risk assessment.

Security Maturity: The level of cybersecurity readiness and resilience of an organization.

Scheduling and Deployment: Software vendors release security patches on a regular schedule. Applicable patches will be tested and validated by IS prior to deployment to campus. Once validated, IS will schedule and deploy validated patches to end points monthly. Communication to campus regarding deployed security patches will be done through Pilots announcements.

System Development Life Cycle (SDLC): A structured process that outlines the steps involved in developing, deploying, and maintaining systems within an organization.

Section 4: Roles & Responsibilities

Account Administrators: Account administrators are an optional subset of the account manager role and do not set policies or procedures. If no separate account administrator exists, these responsibilities default to the account manager.

Account Manager: Account managers oversee the administration of accounts and act as custodians of protected data.

Change Management Committee: The Change Management Committee meets at least once a month to review proposed system changes, assess interactions between systems, and address any identified concerns.

Chief Information Security Officer (CISO): Responsible for overseeing the implementation and enforcement of this policy.

Data Custodian: Implements technical and physical safeguards, documents procedures, and provisions or de-provisions access to institutional data.

Data Steward: Assigns classifications to institutional data, approves operational standards, and defines access criteria.

Developers: Responsible for building systems according to the project's specifications and conducting security testing.

Director of Information Security: Develops and implements the SnowBe Online-wide Information Security Program and coordinates responses to security incidents.

Employees: Adhere to the security policy and complete mandatory security training. Report any security incidents immediately.

Executive Management: has established the overall approach to governance and control.

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

Project Managers: Oversee the SDLC process and ensure adherence to this policy.

Quality Assurance Team: Conduct thorough testing, including security assessments, to ensure system integrity.

Section 5: Statement of Policies, Standards and Procedures

Policies:

SP – 1 Access Control Policy: The rule defines the framework and procedures for managing and limiting access to an organization's information systems and resources. It intends to ensure that access is granted only to authorized individuals, based on their roles and responsibilities, while preventing unauthorized access. This policy assists in safeguarding sensitive data, maintaining confidentiality, and reducing the risk of security breaches.

SP-2 Network Security Policy: The rule outlines the measurements and controls required to protect an organization's network infrastructure from internal and external threats. Its purpose is to provide the integrity, confidentiality, and availability of the organization's network resources by enforcing security controls, monitoring traffic, and preventing unauthorized access or cyberattacks.

SP-3 Confidentiality Policy: Rules and regulations regarding the handling of confidential information.

SP-4 Privacy Policy: Rules and regulations regarding data and how it is collected/used.

SP-5 Incident Response Policy: Rules and regulations outlining the procedures to detect, respond to, and mitigate the impact of security incidents or breaches to minimize risks and restore normal operations effectively.

SP-6 Encryption Policy: Rules and regulations governing the use of encryption methods to protect sensitive data during transmission and storage, ensuring confidentiality and compliance with security standards.

SP-7 Account Management Policy: This policy defines mechanisms to create, maintain, and supervise digital identities for electronic transactions. It provides secure provisioning, consistent monitoring, and proper access controls for the protection of organizational systems, applications, and data.

SP-8 Protection of Information at Rest Policy: This policy protects the confidentiality and integrity of all sensitive information stored on company or contractor-owned equipment or services. Data at rest describes data that is being stored in databases or files. It details measures needed to keep data at rest from unauthorized access, alteration, or disclosure.

SP-9 Change Control Management Policy: The policy works to ensure system and application changes get implemented in deliberate transparent and controlled methods which minimize unexpected outages and disruptions. The protection of our user community requires proper change management through deliberate planning alongside clear communication along with continuous system assessment and robust rollback preparations spanning multiple stages of execution.

SP-10 PCI Compliance Policy: This policy guides the importance of protecting payment card data and customer information. Failure to protect this information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of the unit and SnowBe Online. It aims to ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS).

SP – 11 System Development Life Cycle (SDLC): The purpose of this policy is to establish standard procedures for the development and management of systems at SnowBe, ensuring that security and risk management are integral to the system development life cycle.

SP – 12 Patch Management Policy: The purpose of this policy is to ensure that all Organization-owned devices are proactively managed and patched with appropriate security updates. In addition, this policy is intended to instruct and inform the SnowBe community about the change in end-point computing.

SP – 13 Security Maturity Policy: The purpose of this policy is to establish a structured approach to cybersecurity within SnowBe, ensuring a progressing, risk-based security posture. This policy defines the maturity levels of security processes, the responsibilities of business units, and the continuous improvement of framework to enhance SnowBe's security resilience.

AC-1 Policy and Procedure: Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures.

AC-3 Access Enforcement: The aim of this policy is to protect all information system resources and data at SnowBe Online and restrict the access of those resources and data to only authorized individuals and processes as required by the role-based security of the organization. It forces rules that limit access rights to the minimum necessary to achieve legitimate business needs. It also protects the confidentiality, integrity, and availability of the company and customer data.

AC-5 & AC-6 Separation of Duties and Least Privilege: The purpose of this policy is to lower the risk of misuse, fraud, or other unauthorized activity within SnowBe by dividing critical tasks amongst many people (Separation of Duties) and providing the least amount of privileged access to each user, program, and process (Least Privilege). By this approach, there is no single individual or process has too much control, protecting sensitive data and mission-critical systems from errors or malicious actions.

AC-7: Unsuccessful Logon Attempt: This policy establishes guidelines to limit and monitor unsuccessful login attempts to SnowBe systems, ensuring compliance with NIST SP 800-53r5 AC-7.

AC - 8 & AC - 9 System Use Notification & Previous Logon Notification: This policy ensures users are informed of system use requirements and their previous login activity to enhance security. awareness and compliance with NIST SP 800-53r5 AC-8 and AC-9.

AC - 11 & AC - 12 Device Lock & Session Termination: The purpose of this policy is to implement rules and regulations for ending a user session after periodical times. Ending a user's session is critical to the security of the information stored on company machines. In addition, the purpose of this policy is to lock a user's device, in the event they were to leave for a certain amount of time, thus reducing the chances of an intruder accessing systems or data.

AC- 17 Remote Access Control Policy: The purpose of this policy is to define the rules and requirements for connecting to the SnowBe Online network from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages that may result from the unauthorized use of SnowBe Online resources. Damages include the loss of sensitive or SnowBe Online confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred because of those losses.

AC- 18 Wireless Access Control Policy: The purpose of this policy is to define the minimum requirements related to wireless access. This policy is part of the library of SnowBe Online processes that support the State of Florida information security program, which is collectively referred to as the SnowBe Online Information Security Manual, or "SBISM." The SBISM applies to all Departments, Agencies, Commissions, Boards, Bodies, or other instrumentalities of the Executive Branch of SnowBe Online.

AC - 21 Information Sharing: The purpose of the Information Sharing AC Policy is to establish rules for sharing information contained within the systems to protect customer data privacy where

applicable.
CP-9 System Backup: The purpose of this control is to conduct backups of user-level information contained in SnowBe system components frequency and consistent with recovery time and recovery point objectives.

IA-2 Identification and Authentication (Organizational Users): The purpose of this control is to uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-7 Cryptographic Module Authentication: The purpose of this control is to implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

PE-4 Access Control for Transmission: The purpose of this access control is to protect transmitted data from unauthorized access so authorized users remain the only parties who can see or capture the data during transfer.

SC-4 Information in Shared System Resources: The purpose of this access control is to prevent unauthorized and unintended information transfer via shared system resources and stop information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles.

SC-13 Cryptographic Protection: This control aims to establish guidelines for effectively implementing and managing cryptographic mechanisms to safeguard sensitive information within an information system, protecting it from unauthorized access, tampering, and disclosure by utilizing encryption and other cryptographic techniques.

SC-28 Protection of Information at Rest: This control protects data at rest through safeguards which include encryption methods combined with physical security measures against unauthorized access.

SI-7 Software, Firmware, and Information Integrity: The purpose of this control is to ensure that the software, firmware, and information integrity are implemented based on SnowBe devices and applications to meet the system requirements and objectives.

Standards and Procedures:

P-1 New Account Creation: This policy establishes the timing and process around creating accounts by which members of the community are authenticated and authorized to use SnowBe Online information technology resources. The procedures for creating accounts vary by category and role of each user and the differences and time frames are described within the policy. Procedures for handling individual separations from the SnowBe Online vary based on whether or not the separation is routine. 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.

P-2 Password Procedure: The purpose of this procedure is to show the necessary steps and things needed to set a password on the system for employees and customers. This will ensure top security needed to protect an account on the system.

S-1 Password Standard: This standard identifies the minimum password requirements needed to protect SnowBe Online data and systems. Passwords are used on SnowBe Online devices and systems to facilitate authentication, i.e. helping ensure that the person is who they say they are. The security of SnowBe Online data is highly dependent upon the secrecy and characteristics of the password. Compromised passwords can result in loss of data, denial of service for other users, or attacks directed at other Internet users from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of private data such as private customers data, research participant data, and private employee data

Section 6: Exceptions/Exemptions

Exceptions or exemptions to this plan will be considered on a case-by-case basis and must go via a formal approval process. Each request must include adequate reason and will be subject to review by the IT Director under the guidance of the SnowBe Online IT Manager. Approval is not guaranteed, and all granted exceptions or exemptions will be documented with clearly defined terms, including the specific duration for which the exception or exemption will remain in place. Periodic reviews will be conducted to assess the continued validity, appropriateness, and need for renewal or termination of all exceptions and exemptions.

Section 7: Version History Table

Version	**Date**	**Description**
1.0	03/30/25	Added SDLC policy.
2.0	03/30/25	Added Patch Management Policy.
3.0	03/30/25	Added Security Maturity Policy
4.0	03/30/25	Added roles, definitions, citiations,

Citations

1- Michigan Technological University. (2011). Information security plan. Retrieved from https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf?
2- Howard University. (2019). Information security plan. Retrieved from https://technology.howard.edu/sites/technology.howard.edu/files/202003/Information_Security_Plan_0.pdf?
3- Washington and Lee University. Information Security Plan: Washington and Lee University. (n.d.). Retrieved from https://my.wlu.edu/its/about-its/information-security-plan
4- University of Northern Colorado. (n.d.). Information security roles and responsibilities. Retrieved January 8, 2025, from https://www.unco.edu/informationmanagementtechnology/about/unc_imt_information_security.pdf
5- University of Connecticut. (2021, 08 30). Uconn.Edu. Retrieved from Data Roles and Responsibility Policy: form https://policy.uconn.edu/2012/06/21/data-roles-and-
6- Information Security Plan : Washington and Lee University. Washington and Lee University.

(n.d.). form https://my.wlu.edu/its/about-its/information-security-plan
7- National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5
8. - University of Portland. (n.d.). *Patch management policy*. https://www.up.edu/is/files/policy-patchmanagement.pdf
9. Georgia Technology Authority. (n.d.). *Cybersecurity capability maturity model (SS-20-001)*. https://gta-psg.georgia.gov/psg/cybersecurity-capability-maturity-model-ss-20-001