SNOWBE SECURITY PLAN

Group Member Names:
Phillip White

Version 1.0
Date: November 19, 2023

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 security policies and procedures that support SnowBe's goals and objectives, and to allow SnowBe to satisfy its legal and ethical responsibilities regarding its IT resources.

Information security policies and procedures represent the foundation for SnowBe's ISP. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout SnowBe.

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 the operations of the business. When consistently applied throughout SnowBe, these policies and procedures ensure that information technology resources are protected from a range of threats in order to ensure business continuity and maximize the return on investments of business interests.

This plan reflects SnowBe'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.

Section 2: Scope

This security plan applies to all employees, contractors, and visitors of the organization who have access to SnowBe information technology resources. Such assets include data, images, text, or software, stored on hardware, paper, or other storage media. It covers all aspects of security, including physical security, information security, and personnel security.

Section 3: Definitions

Access Control:
A process for restricting access to systems and data to authorized users.

Access Management:
A framework and set of policies and procedures that ensures that only authorized users and entities have access to the resources they need to perform their authorized tasks. It is a critical component of cybersecurity that helps to protect sensitive data, systems, and applications from unauthorized access, use, disclosure, disruption, modification, or destruction.

Critical Incident:
Is an event that has the potential to cause significant damage to SnowBe's infrastructure, data, or reputation. Critical incidents can be caused by a variety of factors such as data breaches,

ransomware attacks, system failures, power outages, natural disasters, and human error. Critical incidents can have a significant impact on SnowBe's operations, finances, and customer relationships.

Cryptographic:
Refers to the use of mathematical techniques to transform information into a secure form that is difficult or impossible for unauthorized parties to read or modify. It is a fundamental component of cybersecurity, ensuring the confidentiality, integrity, and authenticity of information.

Data Security:
The process of protecting digital data from unauthorized access, corruption, or theft. It encompasses a wide range of practices and technologies.

General Data Protection Regulation (GDPR):
The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Password:
A secret sequence of characters used to verify the identity of a user attempting to access company systems, applications, or data. It serves as a crucial security measure to protect sensitive information from unauthorized access.

Patch Management:
The process of identifying, acquiring, testing, and installing patches or updates to software and devices to fix bugs, close security vulnerabilities, and enhance functionality. It is a critical aspect of cybersecurity and IT operations, as it helps to protect systems from vulnerabilities that could be exploited by cybercriminals.

Payment Card Industry Data Security Standard (PCI_DSS):
The PCI-DSS is a widely accepted set of security requirements designed to protect cardholder data from theft or misuse. Any organization that processes, stores, or transmits cardholder must comply with PCI-DSS in order to accept credit and debit cards.

Principle of Least Privilege:
A fundamental security concept that states that each user or entity should only be granted the minimum level of access necessary to perform their authorized tasks. This principle aims to minimize the potential damage that can occur if a user's account is compromised or if malicious software gains access to a system.

Separation of Duties (SoD):
A control mechanism that divides a task or transaction into several distinct steps and assigns each step to a different person or role. This principle aims to prevent any single individual from having excessive control over a task or transaction, thereby reducing the risk of fraud, error, or abuse of authority.

Web Proxy:
An intermediary server that sits between your computer and the internet. When you request a web page, your computer first sends the request to the proxy server. The proxy server then retrieves the web page from the internet and delivers it to your computer.

Section 4: Roles & Responsibilities

Chief Information Officer (CIO):
The Office of the Chief Information Officer has overall responsibility for the security of SnowBe's information technologies. Implementation of security policies is delegated throughout SnowBe to various SnowBe services; departments, and other units; and to individual users of SnowBe IT resources.

Critical Incident Readiness Team (CIRT):
CIRT is responsible for providing rapid, systematic, and coordinated early intervention in critical incidents. CIRT works with the President and other SnowBe leaders to address critical incidents.

Data Custodian:
The data custodian is the individual or entity (including outsourced services) in possession or control of data and is responsible for safeguarding the data according to the policies and procedures established by the associated data steward. The appropriate level of protection is based on the SnowBe Data Classification policy and the Minimum-Security Standards for Protected Data.

Data Protection Officer (DPO):
Responsible for ensuring that SnowBe is compliant with GDPR. The DPO should:

- Provide advice and guidance to the organization and its employees on the requirements of the GDPR.
- Monitor the organization's compliance.
- Be consulted and provide advice during Data Protection Impact Assessments.
- Be the point of contact for data subjects and for cooperating and consulting with national supervisory authorities, such as the Information Commissioner's Office.
- DPOs should also take responsibility for carrying out data audits and oversee the implementation of compliance tools.

Data Steward:
SnowBe office represented by an executive officer. The data steward has policy-level and planning responsibilities for data owned by SnowBe in their functional areas. Data stewards, as a group, are responsible for recommending policies and establishing procedures and guidelines for SnowBe-wide data administration activities. Data stewards may delegate the implementation of SnowBe policies, standards, and guidelines to data custodians.

Data User:
The data user, synonymous with user, is the individual, automated application or process that is authorized by the data steward to create, enter, edit, and access data, in accordance with the data steward's policies and procedures. Users have a responsibility to:

- Maintain the security of passwords, personal identification numbers (PINs), authentication tokens, and certificates; and will be held accountable for any activities linked to their accounts.
- Manage all forms of authentication and security controls for information processing systems based on the Minimum-Security Standards for Protected Data.
- Use the data only for the purpose specified by the data steward.

- Comply with controls established by the data steward.
- Prevent disclosure of confidential or sensitive data.
- Report suspected security incidents that may have breached the confidentiality of data.

Departments and Other Units:
Departments and other units are responsible for securing any information they create, manage, or store, and for any information, they acquire or access from other SnowBe systems (e.g., PCI data, personnel records, business information). This responsibility includes completing periodic risk assessments, developing, and implementing appropriate security practices, and complying with all aspects of this policy.

Director Endpoint Protection and Identity and Access Management:
This role is responsible for ensuring various aspects of SnowBe's Endpoint Protection and Identity and Access management:

- Ensuring that SnowBe's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the organization from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- Ensuring that SnowBe's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.
- Ensuring that SnowBe's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible.

Director of Information Security:

This role is responsible for ensuring various aspects of SnowBe's cyber and information security:

- Ensuring that SnowBe's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the organization from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- Ensuring that SnowBe's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries and report instances of suspicious and unauthorized events as expeditiously as possible.
- Ensuring that SnowBe's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible.
- Ensuring that SnowBe's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities.

Individuals Using Personally Owned Computers and Other Network Devices:
Team members who use personally owned systems to access SnowBe resources are responsible for the security of their personally owned computers or other network devices and are subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by IT Services for SnowBe computing and network facilities.
- All other laws, regulations, or policies directed at the individual user.

IT Security and Policies Team:
IT security and policies team is responsible for ensuring the security of the provided IT services. The security and policy team must make sure that all intellectual property and proprietary information are protected. This role is responsible for taking all necessary precautions to ensure the security of the services provided by SnowBe.

Other Registered Entities:
Any entity that is a registered user and connected to the SnowBe network is responsible for the security of its computers and network devices and is subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by IT Services for SnowBe computing and network facilities.
- All other laws, regulations, or policies are directed at the organization and its individual users.

Third-Party Vendors:
Third-party vendors providing hosted services and vendors providing support, whether on-premise or from a remote location, are subject to SnowBe security policies and will be required to acknowledge this in the contractual agreements. The vendors are subject to the same auditing and risk assessment requirements as departments, and other units. All contracts, audits, and risk assessments involving third-party vendors will be reviewed and approved by the SnowBe Data Steward based on their area of responsibility.

Section 5: Statement of Policies, Standards and Procedures

Policies:

SP-1 PCI-DSS:
SnowBe is committed to compliance with the Payment Card Industry Data Security Standards (PCI DSS) to protect payment card data regardless of where that data is processed or stored. All team members of SnowBe Online must adhere to these standards to protect our customers and maintain the ability to process payments using payment cards. SnowBe prohibits the retention of complete payment card primary account numbers (PAN) or sensitive authentication data in any system, database, network, computer, tablet, cell phone, or paper file. Storing truncated numbers, in approved formats (first six digits or last four digits) is permissible.

SP-2 Data Security:
SnowBe is committed to protecting the confidentiality, integrity, and availability of all data in its possession, regardless of where it is stored or processed. This policy outlines the minimum security requirements that must be implemented and maintained by all employees, contractors, and other third parties who have access to SnowBe data.

SP-3 Web Proxy:
SnowBe is committed to protecting its network and data from unauthorized access, use, disclosure, disruption, modification, or destruction. This policy outlines the minimum security requirements for the use of web proxy servers at SnowBe.

SP-4 Access Management: (Reserved)

SP-5 Patch Management: (Reserved)

SP-6 Change Control Management:

This policy directs the way that SnowBe manages changes that occur in our technology platforms, systems, and services (in-house and off-site) in a way that is designed to minimize the risk and impact to SnowBe, by ensuring that changes are reasonably controlled.

AC-3 Access Enforcement:

This policy defines the access control requirements for all information systems and data owned or operated by SnowBe.

AC-5 Separation of Duties:

This policy establishes the requirements for separation of duties (SoD) to protect the SnowBe's information systems and data. SoD is a security control that reduces the risk of unauthorized access, modification, or destruction of information systems and data by requiring that no single individual has the capability to perform all the steps necessary to complete a critical task.

MP-5 Media Transport:

This policy will set forth the requirements for transferring or communicating information based on its sensitivity. Data stewards, or their assigned representatives, may designate additional controls to further restrict access to, or to further protect, information.

SC-13 Cryptographic Protection:

Information is an asset and access to it must be managed with care to ensure that confidentiality, integrity, and availability are maintained. Encryption of information and devices helps mitigate the risk of unauthorized interception, disclosure, and access. SnowBe uses encryption to secure information and data while stored, processed, and handled, protect user credentials, and enable secure communications. This policy outlines SnowBe’s approach to cryptographic control management and provides the requirements and responsibilities to ensure information, security, and data governance objectives are met.

Standards and Procedures:

PR-1 New Account Creation Procedure:

This procedure details the steps, information, and considerations that are part of account creation by the SnowBe IT division.

PR-2 Password Procedure:

To establish a standard for the creation, protection, and frequency of change of passwords to safeguard sensitive information and protect against unauthorized access to systems and networks.

STD-1 Password Standard:

To establish a standard for the creation, use, and storage of passwords in order to protect SnowBe’s computer systems and data from unauthorized access.

Section 6: Exceptions/Exemptions

Exceptions:

- An exception is a deviation from a policy that is granted on a case-by-case basis. Exceptions may be granted for the following reasons:
  - A compelling business need that cannot be met without violating the policy.
  - A technical constraint that prevents compliance with the policy
  - A legal or regulatory requirement that conflicts with the policy.

Exemptions:

- An exemption is a blanket waiver from a policy that applies to a specific group of people, systems, or processes. Exemptions may be granted for the following reasons:
  - The group of people, systems, or processes is not subject to the risks that the policy is designed to mitigate.
  - The group of people, systems, or processes is already subject to equivalent or superior controls.
  - The cost of complying with the policy would outweigh the benefits.

Process for requesting an Exception or Exemption:

- To make a request, please submit a written (snail mail or email) request to the appropriate policy owner. The request should include the following information:
  - The specific policy that you are requesting an exception or exemption from.
  - The reason for the request.
  - The proposed alternative controls if any.
  - The duration of the exception or exemption.

Reviewing and Granting Exceptions or Exemptions:

- The policy owner will review the request and make a decision based on the following factors:
  - The severity of the risk that the policy is designed to mitigate.
  - The likelihood that the risk will materialize.
  - The impact of the risk if it materializes.
  - The effectiveness of the proposed alternative controls.
  - The cost of complying with the policy.

The policy owner may grant the exception or exemption, deny the request, or request additional information.

Documentation:

All exceptions and exemptions must be documented in writing and should include the following information:

- The specific policy that the exception or exemption applies to.
- The reason for the exception or exemption.
- The proposed alternative controls if any.
- The duration of the exception or exemption.
- The name of the person who granted the exception or exemption.

Review:
All exceptions and exemptions will be reviewed annually and revoked if they are no longer necessary.

Section 7: Version History Table

Version	Date	Description
1.0	October 30, 2023	Initial draft
1.0	November 2, 2023	Added and edited
1.0	November 3, 2023	Added definitions for PCI-DSS, GDPR, and critical incident, corrected formatting, alphabetized roles, added PCI-DSS as SP-1, moved policy numbers in front of policy name
1.0	November 5, 2023	Added definitions for access management, patch management, web proxy, data security, least privilege, access control, and SoD. Added SP-8 & SP-9. Corrected formatting & update citations.
1.0	November 7, 2023	Formatting corrected
1.0	November 10, 2023	Roles & Responsibilities alphabetized, SP-8 changed to AC-5, SP-9 changed to AC-3, definitions alphabetized, formatting corrected, removed content from standards & procedures.
1.0	November 13, 2023	Removed SP-6 & SP-7 documents not received, Added SP-6 Change Control, added PR-1 account creation, formatting adjusted.
1.0	November 15, 2023	Added PR-2 & STD-1, formatting adjusted, added password definition
1.0	November 19, 2023	SP-4 & SP-5 place holder material changed to (Reserved). Formatting adjusted

Citations

https://security.it.iastate.edu/policies/it-security-plan

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://g.co/bard/share/a167111f22f0

https://g.co/bard/share/bb6b748c58a2

https://g.co/bard/share/efb8e83de49c