SNOWBE ONLINE SECURITY PLAN

Member Names:
Alex Fhermaye
Jake Miranda
Garrett Cole

Version # 1.5
June 30, 2024

Table of Contents

Section 1: Introduction

The purpose of this Security Plan is to provide an overview of the framework and measures necessary to protect the confidentiality, integrity, and availability of SnowBe's information assets and technology infrastructure. This plan contains the strategies, policies, and procedures required to safeguard against security threats, minimize risks, and ensure compliance with applicable legal, regulatory, and industry standards.

Section 2: Scope

This plan is comprehensive in scope and applies to the entire SnowBe Online community. This includes, but is not limited to, Directors, Department Heads, Team Leads, employees, temporary employees, contractors, volunteers, and guests who have access to any of SnowBe Online's information technology resources. These resources encompass a wide range of assets critical to our operations and security.

Information technology resources include, but are not limited to, all forms of data, images, text, and software. These may be stored on various types of hardware such as servers, workstations, laptops, mobile devices, and other electronic devices.

The protection of these assets is paramount to ensuring the confidentiality, integrity, and availability of information, which are the cornerstones of our security posture. This plan sets forth the guidelines and procedures for safeguarding these assets against unauthorized access, disclosure, alteration, and destruction. It is designed to be comprehensive, covering all possible scenarios and providing a clear framework for maintaining and enhancing our information security measures.

Every member of the SnowBe Online community is responsible for understanding and adhering to these guidelines. This responsibility includes recognizing the importance of these resources and the role each individual play in protecting them. By following this plan, we collectively contribute to maintaining the trust of our clients, partners, and stakeholders, and to ensuring the smooth and secure operation of our business processes.

This plan is not static; it is reviewed and updated regularly to adapt to new security challenges and technological advancements. All changes will be communicated promptly to ensure that every member of our community is aware of their responsibilities and the importance of compliance. By adhering to this plan, we uphold SnowBe Online's commitment to excellence in information security.

Section 3: Definitions

Access Controls:
Security techniques and measures that regulate who or what can view or use resources in a computing environment.

Availability:
The assurance that information and resources are accessible to authorized users when needed.

Compliance:
The act of adhering to and demonstrating adherence to laws, regulations, guidelines, and specifications relevant to its business processes.

Confidentiality:
The assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Information Assets:
Data, images, text, or software stored on hardware, paper, or other storage media that hold value to SnowBe Online.

Integrity:
The assurance that information is accurate, complete, and has not been altered in an unauthorized manner.

IT Security Exception Request Form:
A formal document used to request deviations from established IT security policies.

Legal, Regulatory, and Industry Standards:
Set of laws, regulations, guidelines, and specifications established by regulatory authorities or industry groups to ensure security, privacy, and operational efficiency.

NIST 800-53:
A publication that provides a catalog of security and privacy controls for federal information systems and organizations.

Patch:
A piece of software designed to update or fix problems with a computer program or its supporting data, including fixing security vulnerabilities and other bugs.

PCI DSS (Payment Card Industry Data Security Standard):
A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

Risk Assessments:
The process of identifying, evaluating, and estimating the levels of risk involved in a situation, followed by coordinated efforts to mitigate and manage the risk.

Security Controls:

Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Security Incidents:

Events that indicate that an organization's systems or data may have been compromised or that measures put in place to protect them may have failed.

Security Posture:

The overall security status of an organization's software, hardware, services, networks, information, and systems.

Security Threats:

Potential events or actions that could cause harm to information systems through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Technology Infrastructure:

The composite hardware, software, network resources, and services required for the existence, operation, and management of an enterprise IT environment.

Section 4: Roles & Responsibilities

Chief Information Officer (CIO)

- Develop and implement the overall IT security strategy in alignment with business objectives.
- Oversee the IT department to ensure effective execution of security policies and controls.
- Ensure compliance with industry standards and regulatory requirements, including NIST 800-53 and PCI DSS.

Compliance Officer

- Ensure the company adheres to all relevant legal, regulatory, and industry standards.
- Conduct regular audits and assessments to identify compliance gaps.
- Work with other departments to implement corrective actions and maintain compliance.

IT Consultant

- Provide expert advice and guidance on IT security best practices and frameworks.
- Conduct risk assessments and develop action plans to address identified vulnerabilities.
- Assist in the implementation of security controls, policies, and procedures.

IT Security Manager

- Oversee the day-to-day operations of IT security within the company.
- Manage the IT security team and ensure the implementation of security controls and measures.
- Monitor security incidents and respond to breaches or threats.

Sales Team

- Adhere to IT security policies and procedures, particularly when accessing company systems remotely.
- Report any suspicious activities or potential security incidents to the IT security team.
- Ensure the secure handling of customer data and payment information during transactions.

System Administrator

- Manage and maintain servers, ensuring they are secure and up-to-date.
- Implement and enforce access controls to limit data access based on roles and responsibilities.
- Regularly update and patch operating systems and software to mitigate vulnerabilities.

Web Developer

- Ensure the company's website and applications are secure and up-to-date.
- Implement security measures for online transactions and data storage.
- Regularly update and patch the WordPress shopping cart and other web components.

Section 5: Statement of Policies, Standards and Procedures

Policies

11.1 Access Control:

A set of rules and procedures designed to regulate who can view or use resources in a computing environment, ensuring that only authorized users have access to specific data and systems.

11.2 Account Management:

Is a set of guidelines and procedures for creating, maintaining, and securing user accounts to ensure proper access control and accountability within an organization.

11.3 Audit Logging and Monitoring:

Establishes requirements for logging and monitoring user activities, system events, and security incidents. It ensures that logs are reviewed regularly, anomalies are investigated, and records are retained for a defined period to support forensic analysis.

11.4 Data Privacy:

Is a framework of guidelines and practices designed to protect personal and sensitive information from unauthorized access, use, and disclosure, ensuring compliance with legal and regulatory requirements.

11.40 Payment Card Industry (PCI) Compliance:

Refers to the adherence to a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

11.5 Security Awareness and Training:

Establishes a program for educating employees about security policies, procedures, and best practices. It covers topics such as phishing, social engineering, password security, and data protection to enhance overall security awareness.

11.6 Wireless Access:

Is a set of rules and procedures governing the secure use and management of wireless networks within an organization to prevent unauthorized access and protect data integrity.

11.7 Unsuccessful Logon Attempts:

Monitors and limits the number of failed login attempts to prevent unauthorized access and alert administrators to potential security threats.

11.8 Remote Access:

Manages and secures the ability for users to access a company's network and resources from locations outside the physical premises, often using VPNs and multi-factor authentication.

11.10 Access Enforcement:

Ensures that access to systems and data is granted based on predefined policies and roles, restricting users to only the resources they are authorized to use.

11.11 Session Termination:

Automatically ends user sessions after a specified period of inactivity or at the end of a work session to prevent unauthorized access and protect sensitive information.

11.12 Change Control Management:

Outlines procedures and guidelines for managing changes to systems, software, or processes within an organization. It typically includes steps for requesting, approving, implementing, and reviewing changes to ensure they are properly assessed, tested, and documented.

Standards and Procedures

11.13 New Account Procedure:

Governs the process of creating and managing user accounts within an organization's IT systems. It defines the steps required to request, approve, create, modify, and deactivate user accounts, emphasizing security and compliance with access control policies.

11.14 Password Standard

Defines the requirements and best practices for password creation and management to ensure security. This includes criteria such as minimum length, complexity (use of upper- and lower-case letters, numbers, and special characters), and prohibited elements (e.g., common words or easily guessable sequences). It also sets guidelines for password expiration, reuse limitations, and multi-factor authentication to enhance security.

11.15 Password Procedure

Outlines the steps and guidelines for creating, using, and managing passwords within an organization. It includes instructions for selecting strong passwords, changing them regularly, and securely storing them. The procedure also covers the process for recovering or resetting forgotten passwords and the protocols for responding to suspected password breaches.

Section 6: Exceptions/Exemptions

At SnowBe Online, we recognize that there may be exceptional circumstances requiring deviations from our established IT security policies. However, such exceptions/exemptions are not guaranteed approval and must be carefully evaluated to ensure they do not compromise our security posture. The following outlines the process for requesting and managing exceptions/exemptions:

How to Request an Exception/Exemption

1. All requests for exceptions or exemptions must be submitted in writing via the official IT Security Exception Request Form, available on the company net.

2. A detailed explanation of why the exception or exemption is being requested, including the specific policy or control from which the deviation is sought. The proposed duration for which the exception or exemption is needed.

Approval Process

1. The IT Security Manager will review the request to ensure it includes all required information and assess the potential risks and impacts.

2. The Chief Information Officer (CIO) has the final authority to approve or deny exceptions and exemptions. In cases involving significant risk, the CIO may consult with the Chief Executive Officer (CEO) or the IT Security Advisory Committee.

3. The applicant will be notified in writing of the decision, including any conditions or additional controls required as part of the approval.

Duration and Review

1. Approved exceptions or exemptions will typically be granted for a specified duration, not exceeding one year unless otherwise stated.

2. All active exceptions or exemptions will be reviewed periodically by the IT Security Manager to ensure that they remain necessary and that any associated risks are being adequately managed.

Section 7: Version History Table

Version	Date	Description
1.0	June 4, 2024	First Submission/Review
1.1	June 10, 2024	Updated Plan
1.2	June 15, 2024	Updated Plan 2 (Minor Corrections)
1.3	June 17, 2024	Added security control policies
1.4	June 24, 2024	Added a policy and a standard
1.5	June 30, 2024	Added Password Procedure and Standard

Citations

Information security plan. (n.d.). https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

Data security plan. (n.d.-a). https://www.ayadata.ai/wp-content/uploads/2023/07/AyaDATA_Data-Security-Plan_V001.pdf

Information security roles and responsibilities policy. Sourcegraph handbook. (n.d.). https://handbook.sourcegraph.com/company-info-and-process/policies/information-security-roles-and-responsibilities/

It/information security exception request process. Information Security. (n.d.). https://security.calpoly.edu/content/exception-process

Exception management. Infosec. (n.d.). https://www.infosecinstitute.com/resources/management-compliance-auditing/exception-management/