SNOWBE ONLINE SECURITY PLAN

Group Member Names:
Pedro Portillo, Lance Belton, Lana Basdeo

Version 1 Date 4/22/2024

Table of Contents

Section 1: Introduction

SnowBe Online is a lifestyle brand dedicated to providing excellent products to beach and snow enthusiasts while ensuring their safety and security in the digital world. Their goal is to implement a strong security strategy to safeguard personal information and transactional data while adhering to industry regulations and best practices. They continuously monitor and train to detect, audit, and control potential security risks. SnowBe Online prioritizes security to establish trust and foster long-term relationships with customers. They want to make the digital environment safer for beach and snow enthusiasts.

Section 2: Scope

SnowBe Online's new security plan covers all aspects of our operations, systems, and processes, ensuring comprehensive data protection for our customers, infrastructure integrity, and business continuity.

Section 3: Definitions

- **Compliance:** the act of obeying a law or rule, especially one that controls a particular industry or type of work.

- **Compliance Standards:** A list of guidelines or regulations that must be followed to ensure the company meets industry best practices and standards**.**

- **CISO (Chief Information Security Officer):** The ISO is a senior-level executive responsible for overseeing an organization's information security program, ensuring adequate protection of information assets and technologies.

- **Exceptions/Exemptions:** Security policies can be categorized into exceptions and exemptions, where specific rules or requirements are not applied due to specific circumstances or considerations.

- **Escalation Process:** An escalation process is a process that involves raising issues or concerns to higher management or specialized teams for resolution when they cannot be resolved at lower levels.

- **Least Privilege:** This principle restricts users’ access rights to the minimum levels required to perform their tasks, reducing the potential impact of a security breach.

- **Mitigating Factors:** Circumstances or conditions that lessen the severity or impact of a situation, often used in risk assessment to determine appropriate responses.

- **Phishing:** A cyber-attack that is used by sending fraudulent emails, text messages, or websites to trick people into giving their private information to attackers.

- **Risk Management:** The identification, assessment, and mitigation of potential threats or vulnerabilities that may jeopardize the organization's goals or operations.

- **Vendor Risk Management:** This involves assessing and managing the potential risks associated with third-party vendors or suppliers who have access to an organization's systems or data.

- **Incident Response Plans:** These are documented procedures for responding to cybersecurity incidents such as data breaches, malware infections, or network intrusions.

- **Two-Factor Authentication (2FA):** 2FA is an authentication method that requires users to provide two different forms of identification before granting access to a system or application.

- **Penetration Testing:** This is a simulated cyber-attack against a computer system, network, or application to identify security weaknesses and vulnerabilities.

Section 4: Roles & Responsibilities

- **Employees:** Employees at SnowBe are responsible for information security, data protection, access control, security incident reporting, device security, physical security, and compliance with laws, regulations, and industry standards. They must stay informed about security policies, handle sensitive information appropriately, protect login credentials, report security incidents, and adhere to physical security measures.

- **Data Steward:** Responsible for developing and implementing data governance policies, maintaining data quality standards, classifying data based on sensitivity, establishing access control mechanisms, and ensuring compliance with data privacy regulations. This includes collaborating with IT security teams to establish role-based access control and facilitating data privacy impact assessments. The goal is to ensure data assets are managed effectively and protected.

- **CISO (Chief Information Security Officer):** The Chief Information Security Officer (CISO) at SnowBe is responsible for overseeing the organization's information security program. They develop and implement an information security strategy, enforce policies, manage risks, ensure compliance with laws and regulations, develop, and maintain incident response plans, promote security awareness and training, oversee security architecture, and design, and manage vendor risk. The ISO ensures SnowBe's information assets are protected and that security measures are integrated into the organization's IT infrastructure. They also manage vendor risks, evaluating practices, conducting due diligence, and establishing contractual requirements for security controls and protections. The ISO's role is crucial in ensuring SnowBe's overall security posture.

- **IT Security Team:** An IT security team at SnowBe protects the organization's information assets, infrastructure, and systems from cybersecurity threats. They develop and implement cybersecurity strategies, monitor networks, manage incident response, perform vulnerability assessments, conduct security awareness programs, and manage user identities and access rights. They also ensure a culture of security awareness.

- **Third-Party Vendors:** Third-party vendors that provide hosted services and support, whether on campus or remotely, are subject to SnowBe Online security policies and must acknowledge this in their contractual agreements. Vendors are held to the same auditing and risk assessment standards as colleges, departments, and other units. All contracts, audits, and risk assessments involving third-party vendors will be reviewed and approved by the company Data Steward in accordance with their area of responsibility.

Section 5: Statement of Policies, Standards and Procedures

Policies:

POL-001: Password Policy

This policy aims to establish a standard for creating strong passwords, protecting them, and ensuring that they are changed regularly. It applies to all personnel in charge of accounts on any system, including those with network access or non-public information. Passwords should not be entered into electronic communication and must follow guidelines. Common applications include user accounts, web accounts, email accounts, screen saver protection, voicemail passwords, and local router logins.

POL-002: Security Awareness Training Policy

A Security Training and Awareness Policy is a guideline created to educate employees about security best practices and raising awareness of potential risks within an organization. It includes guidelines for conducting regular training sessions, defining roles and responsibilities of stakeholders, and emphasizing ongoing communication and reinforcement of security protocols. The policy also addresses an employee’s ability to implement measures to address gaps in knowledge. This policy creates a culture of security awareness and accountability.

POL-003: Data Classification Policy

This idea is relevant because, at its core, data categorization policies provide the framework for safeguarding the information created, saved, processed, and transferred inside an enterprise. It provides the framework for creating the rules, guidelines, and security measures required to protect sensitive data.

POL-004: Log Management Policy

This log management and review policy defines specific requirements for information systems to generate, store, process, and aggregate appropriate audit logs across the organization's entire environment to provide key information and detect indicators of potential compromise. This policy applies to all information systems within the organization's production network. This policy applies to all employees, contractors, and partners of the organization that administer or provide maintenance on the organization's production systems. Throughout this policy, these individuals are referred to as system administrators.

POL-005: Backup and Disaster Recovery Policy

A Backup and Disaster Recovery (BDR) policy is a structured plan that outlines how an organization will protect its data, systems, and operations in the event of an unexpected incident or disaster. It seeks to ensure business continuity, safeguard data integrity, and reduce risks. A comprehensive BDR policy includes backup procedures, retention policies, disaster recovery procedures, security measures, documentation, and training, as well as monitoring and testing. Implementing a well-defined BDR policy can help you build resilience, reduce financial losses, and maintain customer trust in the face of unexpected events.

POL-006: Virtual Private Network Acceptable Use Policy

A Virtual Private Network or VPN Acceptable Use Policy is a set of guidelines for authorized use of VPN connections by employees, contractors, and other users. It outlines permissible activities, responsibilities, and security measures to ensure confidentiality, integrity, and availability of organizational resources and data. Key components include defining the purpose, authorized users, permitted use, security measures, data protection, prohibited activities, compliance with laws, monitoring, reporting procedures, and policy review and updates.

POL-007: PCI Policy

The PCI DSS is a set of security standards developed by the PCI Security Standards Council (PCI SSC) to enhance payment account data security. It includes technical and operational requirements for security management, policies, procedures, network architecture, and software design. The standards apply to all organizations that store, process, or transmit cardholder data, preventing credit card fraud and hacking.

AC-3: Account Management

The Account Management (AC-2) policy outlines procedures for managing user accounts within a system, including defining account types, assigning managers, and ensuring access authorizations. It mandates approvals for account creation requests, monitors usage, and authorizes access based on authorization. The policy also mandates automated mechanisms for account management, removal of temporary or emergency accounts, disabling accounts for expiration or inactivity, automated auditing, and immediate disabling of accounts for high-risk users.

AC-5: Separation of Duties

The AC-5 control, or Separation of Duties, is a security framework that requires organizations to identify and document specific duties that require separation and define system access authorizations accordingly. This helps mitigate the risk of unauthorized activities and malicious behavior, especially without collusion. It encompasses both mission and support functions, ensuring distinct individuals perform system support tasks and security personnel do not overlap with audit functions. This framework aligns with other controls like AC-2, AC-3, IA-2, IA-4, and IA-12, enhancing security posture and maintaining accountability.

AC-7: Unsuccessful Logon Attempts

SnowBe will be implementing controls to limit unsuccessful logon attempts, enforce a maximum number of invalid attempts within a specified timeframe, and take automatic actions when this limit is exceeded. These actions could include locking accounts, delaying prompts, notifying system administrators, or using alternative authentication factors. Mobile devices may also be purged or wipe after a defined number of unsuccessful logon attempts. Biometric attempt limiting and alternate authentication factors further strengthen security measures, aligning with established security standards.

AC-6: Least Privilege

The Least Privilege (AC-6) policy mandates the implementation of the principle of least privilege, ensuring that users and processes only have authorized access necessary to accomplish assigned agency tasks. It authorizes access to security functions and security-relevant information for individuals or roles, while requiring non-privileged access for non-security functions. The policy restricts privileged accounts to agency-defined personnel or roles, necessitates regular review of user privileges to validate their necessity, and mandates logging of privileged function usage. Additionally, it prohibits non-privileged users from executing privileged functions, thereby enhancing access control, and minimizing the risk of unauthorized access or misuse within the system.

AC-17: Remote Access

Users can connect to a computer network remotely from locations other than its physical location. It offers flexibility and convenience by enabling the use of technologies such as VPNs or remote desktop protocols to access resources and data as if they were locally stored.

AC-24: Access Control Decision

Access control decisions, which are based on pre-established rules and authentication, decide whether a person or process may access resources. Permissions and credentials are compared against access control policies in these judgments. To protect sensitive information and resources, access is either allowed or restricted based on predetermined criteria.

Standards and Procedures

Section 6: Exceptions/Exemptions

Exceptions:

SnowBe Online requires employees, contractors, or vendors to request exceptions for any aspect of its Security Plan that does not adhere to compliance standards. The Chief Information Security Officer and the relevant Unit Head must approve exception requests, considering risks and mitigating factors. The ISO evaluates exceptions, granting temporary exceptions for up to one year and reviewing annually for renewal. Non-compliant elements of the Security Plan may be subject to corrective actions or removal. If requests are unapproved or expired, they may escalate to the CISO for review.

Exemptions:

SnowBe Online allows exemptions for any aspect of its Security Plan that requires alternative controls, subject to written approval by the CISO and relevant Unit Head. Exemptions are granted for a maximum of one year and must be reviewed annually. Non-compliant elements of the Security Plan may be subject to corrective actions or removal. If unapproved or expired, the matter is escalated to the CISO, who coordinates with IT and functional stakeholders.

Section 7: Version History Table

Version	Date	Description
Version 1.0	4/15/2024	First Draft
Version 2.0	4/22/2024	Access Control Draft

Citations

- *Password Policy*. (n.d.). Retrieved April 15, 2024, from https://cpcstech.com/pdf/password_policy.pdf

- *Central Arkansas Library System*. (n.d.). Central Arkansas Library System. https://cals.org/pci-compliance-policy

- Gamboa, F. (2023, December 1). *Data Classification for Compliance: Looking at the Nuances*. Https://Blog.netwrix.com/. https://blog.netwrix.com/2023/12/01/data-classification-for-compliance/

- *Log Management Policy | Nanonets Security*. (2021, March 16). Nanonets.com. https://security.nanonets.com/log-management-policy#policy

- *Wisconsin Department of Enterprise Technology. (n.d.). Access control standard executive branch. Retrieved from https://det.wi.gov/Documents/100_Access_Control_Standard_Executive_Branch.pdf*