Group 5
Instructor: Robin Alarcon
CYB349-O | C202411-02
November 21, 2024

4.3: Assignment: Security Plan, Policies, Standards, and Procedures

Group Leader: Daphnie
John Bays; Jordan Bedard; Richard Berthelot; Daphnie Bruno
Nicholette Mickelson; Marvena Windom; Lyndsei Wilkins

Week 1

SP-01 – PCI DSS Policy

This policy provides guidance about 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 SnowBe Online.

SP-02 – Password Policy

This policy is to educate SnowBe Online staff on the characteristics of a strong password as well as to provide recommendations on how to securely maintain and manage passwords. The purpose of this policy is to establish a strong password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

SP-03 – Security Awareness Training Policy

The Security Awareness and Training Policy establishes the requirements to assist Information Technology (IT) system managers, administrators, and users of SnowBe Online systems and data the steps to ensure that SnowBe Online systems and data are appropriately safeguarded. Our executives, staff, vice presidents, interns, managers, senior managers, board members, contractors and business partners are the frontline to protecting SnowBe Online's data assets and this policy will assist at providing consistent guidance and overall approach to security awareness.

SP-04 – Data Retention Policy

This policy is intended to assist SnowBe Online inadequately identifying, protecting, and managing the records it needs to maintain and the process of destroying records that have reached their mandatory retention periods or are no longer necessary for the operations of SnowBe Online. This policy will help ensure that SnowBe complies with all applicable laws and regulations governing records retention and eliminates unnecessary records, which cause storage bloat.

SP-05 – Remote Access Policy

The purpose of this policy is to define standards for connecting to SnowBe Online's network from any end user device, for example: PC, Tablet). These standards are designed to minimize the potential security exposure to SnowBe Online from damages which may result from unauthorized use of SnowBe Online resources. Potential damages include the loss of sensitive or SnowBe Online confidential data, intellectual property, damage to public image, and damage to critical SnowBe Online internal systems.

SP-06 – Acceptable Usage Policy

The purpose of this policy is to establish what behaviors are acceptable with company devices and on the company network. These guidelines will help to mitigate risk against cyber incidents. This policy will also mitigate risk against behaviors that would cause damage to the company's image.

SP-07 – Third Party Vendor Security Policy

The purpose of this policy is to ensure that third-party vendors working with SnowBe Online adhere to our security, data protection, and compliance standards to safeguard customer and company information. This policy outlines the requirements, processes, and responsibilities for the management and oversight of third-party vendor relationships, especially those with access to sensitive data or critical systems. It includes rules to assess, monitor, and manage risks associated with these relationships.

SP-08 - Customer Privacy Policy

The purpose of this policy is to establish SnowBe Online's commitment to protecting the privacy of our customers. This document outlines how we collect, use, store, and protect personally identifiable information (PII). Our goal is to be transparent about our data handling practices and to ensure compliance with applicable privacy laws and regulations. By implementing this policy, SnowBe aims to build and maintain the trust of our customers, especially as our business operations rely heavily on online sales and customer interactions.

SP-09 – Incident Reporting Policy

Users of SnowBe Online Resources connected to the SnowBe Online network, as well as all users of SnowBe Online Data, must promptly report all actual and suspected Cyber Security Incidents. SnowBe Online IT is responsible for evaluating incidents for a breach of SnowBe Online Data, including Personal Information held by SnowBe Online, and when necessary to initiate the Cyber Security Incident Response Plan. Prompt and consistent reporting of Cyber Security Incidents protects and preserves electronic resources and institutional data and aids SnowBe Online's compliance with applicable law.

SP-10 – Computer and Network Security Policy

This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

SP-11 – Removable Media Policy

This policy establishes the correct practices with using removable media devices

SP-12 – Patch Policy

This document establishes the Vulnerability and Patch Management Policy for SnowBe Online. This policy defines requirements for the management of information security vulnerabilities and the notification, testing, and installation of security-related patches on devices connected to SnowBe Online networks

SP-13 – Electronic Data Disposal Policy

The purpose of this policy is to provide SnowBe associates guidelines for proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices and electronic media being disposed, recycled or transferred either as surplus property or to another user. The disposal procedures used will depend upon the type and intended disposition of the media. This also is relevant for clients, as a promise of how SnowBe Online will be handling their data.

Week 2

AC-01 Policy and Procedures

The purpose of this guide is to provide guidance for the Policy and Procedures controls identified in NIST SP 800-53. The guide provides SnowBe Online employees, contractors with significant security responsibilities and other IT personnel involved in implementing access control, guidance on the specific procedures they are to follow for implementing AC features and functions for systems under their purview.

AC-02 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-03 Access Enforcement

The purpose of this document is to define the Snowbe Online policy and procedures for implementing and maintaining appropriate access controls (see Definitions) for State information assets (see Definitions). This document corresponds to the Access Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53.

AC-04 Information Flow Enforcement

This policy is to establish limits on data access and distribution. This policy ensures that information flows within SnowBe Online's systems are secure, authorized, and compliant with applicable legal and regulatory requirements. By enforcing strict controls over how information is transmitted, accessed, and shared, the policy aims to protect sensitive data, prevent unauthorized access or leakage, and maintain the integrity of business operations.

AC-05 Separation of Duties

This policy is enacted to educate employees on the expectations for dividing key areas of the business. This barrier will reduce the risk of fraud or unauthorized access from other departments.

AC-06 Least Privilege Policy

The purpose of this policy is to establish and enforce the principle of least privilege within SnowBe Online's systems and networks. This policy ensures that users are granted the minimum level of access required to perform their assigned duties, thereby enhancing security.

AC-07 Unsuccessful Logon Attempt Policy

The purpose of this guide is to provide guidance for the Unsuccessful Logon Attempts identified in NIST SP 800-53. This policy provides SnowBe Online employees, contractors with significant security responsibilities and other IT personnel involved in implementing access control, guidance on the specific procedures they are to follow for implementing Unsuccessful Logon Attempts features and functions for systems under their purview.

AC-11 Device Lock

This policy describes the minimum-security policy for mobile devices. Mobile devices must be appropriately secured to Prevent sensitive or confidential data from being lost or compromised Reduce the risk of spreading viruses Mitigate other forms of abuse of the company's computing and information infrastructure.

AC-14 Permitted Actions Without Identification or Authentication

This policy outlines the permitted actions that can be taken without requiring identification or authentication, ensuring that SnowBe Online maintains a balance between security and usability. It aims to define the circumstances under which access to certain resources or data can be granted without the need for formal identification or authentication processes.

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 Policy

This policy establishes the requirements for access control when using mobile devices to access SnowBe's network, systems, and data. It aims to protect company information and customer data by defining rules for mobile device usage and ensuring compliance with security standards.

AC-20 Use of External Systems

The purpose of this policy is to ensure that information shared internally and externally by SnowBe is managed securely. It aims to establish protocols for sharing data to protect customer privacy and prevent unauthorized disclosure of sensitive company information.

AC-21 Information Sharing

The purpose of this policy is to ensure that information shared internally and externally by SnowBe is managed securely. It aims to establish protocols for sharing data to protect customer privacy and prevent unauthorized disclosure of sensitive company information.

AC-25 Reference Monitor

The purpose of this policy is to mediate all access between subjects and objects, enforcing security policies to prevent unauthorized actions such as writing to restricted files or reading top secret information.

Week 3

CM-01 Change Control Management

The purpose of this policy is to ensure that all changes to SnowBe Online IT Resources are tracked, to support continuity of IT services, and reduce negative impact on services and Users.

NU-01 New Account Creation Procedure

This procedure outlines the steps for creating user accounts on SnowBe Online Systems. The purpose of this procedure is to detail the steps involved in establishing new user accounts for both internal employees and external customers. It ensures a consistent account creation process throughout the organization.

Week 4

PP-01 Password Procedure

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of this Procedure is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

PS-01 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 research participant data and private employee data.