SNOWBE ONLINE SECURITY PLAN

Group Member Names:
Michael Kohronas
Xavier Maysonet
Jeremy Wilson

Date: 06/2024
Version #5

Table of Contents

Section 1: Introduction

The purpose of this security plan is to safeguard the confidentiality, integrity, and availability of data, formulate, evolve, and document the information policies and procedures that align with SnowBe Online business goals and objectives.
This plan will enable SnowBe Online to fulfill its legal and ethical responsibilities concerning its IT resources while maintaining the laid-back culture that resonates with its brand identity. It aims to ensure a secure and reliable online shopping experience for our customers, protect sensitive customer and company data, and uphold the trust and reputation that SnowBe Online has built over the years.

Section 2: Scope

This plan applies to all employees and contractors of SnowBe Online. This plan also applies to all individuals and entities who use SnowBe Online's resources including but not limited to, contractors, temporary employees, and volunteers. This Plan is not intended to restrict communications or actions protected or required by applicable law.

This plan provides detailed information security guidance that you must follow in addition to any other relevant documentation. This Plan covers all written, verbal, and digital information held, used or transmitted by or on behalf of the SnowBe Online, irrespective of media. This includes, but is not limited to:

a. paper records.
b. hand-held devices.
c. telephones.
d. information stored on computer systems; and
e. information passed on verbally.

The information covered in this Plan may include:

a. personal data relating to, but not limited to, staff, customers, clients or suppliers.
b. other business information; and
c. confidential, classified, restricted and publicly available information.

This plan applies to the SnowBe Employees, Consultants, On-Prem and AWS Servers, Company Devices, and Data protection.

Section 3: Definitions

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

Access Enforcement: Is the process of ensuring that only authorized users can access certain applications and data.

Access Rights: Level of permissions granted to users to access resources needed to perform daily job.

Authorized User: An individual who has approved access to an information asset to perform job responsibilities.

Backup: A copy of data that can be used to store and recover the data.

Data Classification: Process of organizing data into categories for its most effective and efficient. Identity Theft: Fraud committed or attempted using the identifying information of another person without authority.

Individual Accounts: An individual account is a unique account issued to a single user. The account enables the user to authenticate to systems with a digital identity. After a user is authenticated, the user is authorized or denied access to the system based on the permissions that are assigned directly or indirectly to that user.

Network Security: Covers the implementation and management of network security measures, to include firewalls, IDS/IPS and network segmentation.

Password: A secret word or phrase that must be used to gain admission to something (i.e. a computer system).

Remote Access: Access to an organization information system by user (or a process acting on behalf of a user) communicating through an external network.

Session: A period of interaction between a user and a system.

Section 4: Roles & Responsibilities

Data Stewards: Supervisors who manage user access to data within their departments and enforce security policies.

Employees: Are responsible for using company data and systems securely, adhering to this plan, and reporting suspicious activity.

Executive Management: Provides oversight and leadership for the information security program.

IT Director: Provide overall leadership and direction for IT security plan development and implementation

Section 5: Statement of Policies, Standards and Procedures

Policies

SP – 1 PCI DSS – The purpose of the PCI DSS policy is to ensure that SnowBe can effectively protect cardholder data, use compliant card readers, and properly store transaction history.

SP – 2 Security Training and Awareness Training Policy – The Security Awareness and Training Policy establishes the requirements to assist any staff under SnowBe make smarter online decisions. Our staff is the front line of our security, and this policy will assist in providing training and guidance regarding the best online habits to stay protected. Overall, increasing the security of our staff by promoting safer online habits.

SP – 3 Mobile Device Management (MDM) – The purpose of the Mobile Device Management policy is to protect company data by ensuring safe use of our mobile devices. This aims to protect company data by securing mobile devices.

SP – 4 Physical Security Policy – The Physical Security policy is to maintain security of SnowBe Online facilities, assets and personnel to prevent unauthorized access.

SP – 5 Email Policy – To secure SnowBe Onlines email system from unauthorized access. Outlines all expectations from efficient use to curve the potential of unauthorized access.

SP – 6 Data Classification Policy – To standardize how a company manages its data assets. It ensures that sensitive information is properly handled throughout its entire lifecycle by all relevant stakeholders. This policy significantly reduces risks associated with data security, privacy, and compliance.

SP – 7 Regular Backup Policy – The Purpose of the Regular Backup Policy is to ensure that all critical data and information assets are regularly backed up and can be recovered in case of that loss. This policy is integral to the organization’s business continuity and disaster recovery plan

CM – 3 Configuration Change Control – The purpose of the SnowBe Change Management/Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to SnowBe Information Resources.

AC – 01 Access Control Policy and Procedures – All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the requirements set forth by the State to implement the family of Access Control security controls at the organization, process and/or system level for all information assets / State data.

AC – 02 Account Management – The purpose of this standard is to establish the rules and processes for creating, maintaining, and controlling the access of a digital identity to SnowBe Online Information Technology (IT) resources and assets to protect SnowBe Online data and information.

AC – 03 Access Enforcement – The Access Enforcement Policy is for access to organizational information systems to protect sensitive data, comply with security standards and maintain system integrity.

AC – 05 Separation of Duties – Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

AC – 06 Least Privilege – Least Privilege Access would ensure that employees or users of SnowBe system are permitted only necessary access to information that relates to their job function, increasing security and minimizing security risks.

AC – 11 Account Lock – The Purpose of this policy is to prevent unauthorized access to SnowBe Online's information systems during periods of inactivity. This Policy is designed to automatically lock user session after a predetermined period of inactivity.

AC – 17 Remote Access – The purpose of this policy is to define standards for connecting to SnowBe network from any host outside of SnowBe's corporate network. This policy aims to minimize the potential exposure to SnowBe from damages which may result from unauthorized use of SnowBe resources.

Standards and Procedures

AP – 1 Create New Account Procedure - This procedure details the procedural steps, information, and considerations that are part of account creation and removal by SnowBe's Information Technology department

AP – 2 Password Standard - The purpose of this policy is to ensure that every SnowBe Online employee and contractor takes responsibility for the security of their system access login and password credentials. Adherence to the password standards outlined in this policy is mandatory. Any disclosure or sharing of passwords that contradicts this policy is strictly prohibited at SnowBe Online. This is crucial in maintaining the integrity and security of our systems and data.

AP – 3 Password Procedure - Passwords are an important aspect of computer security. They are the front line of protection for user accounts. This Procedure establishes a standard for creation of strong passwords, their protection, and the frequency of change.

Section 6: Exceptions/Exemptions

Exceptions to this policy will be considered on a case-by-case basis and **do not guarantee approval**. To request an exception, please submit a written request to the **IT Director** outlining the following:

How to Request Exceptions/Exemptions?
To request an Exception or Exemption from a policy that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The **IT Director**, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. **The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions.**
Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement – The failure to comply with policies, standards, or procedures will result in a warning or disciplinary action depending on the severity of the infraction.

Section 7: Version History Table

Version	**Date**	**Description**
#1	06/06/2024	Opened and filled out document. This includes Section 1,2,3,4, & 6
#2	06/10/2024	Added policies to document
#3	06/17/2024	Added AC policies and new definitions

#4	06/25/2024	Added CM – 3 & Account Procedure in the standards and procedure tab
#5	06/27/2024	Added Account Procedure and Account Standard to document

Citations:

Where I found the Intro, Scope and Definitions
https://www.rocketlawyer.com/secure/interview/questions.aspx?document=122436490&id=2645&templateUuid=cceecb34-fad5-4444-a16b-165349ebc118#/q1

Roles & Responsibility
https://www.bowiestate.edu/files/resources/information-security-public.pdf