System Security Plan

SnowBe Corporation

January 28, 2023

Version: 4.0

Table of Contents

Introduction

Information security is essential to the mission of SnowBe and is a company-wide responsibility. The purpose of this document is to provide an overview of the information security program at SnowBe, including the policies and standards that form the foundation of the program. Policies and standards inform the practices taken to protect electronic resources that fall under federal and state laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry, Data Security Standard (PCI-DSS).

The intent of the plan is to provide effective security that aligns with and enables open and collaborative computing environments and business administration in support of all activities that fulfill the mission of SnowBe. The program is intended to assess and manage risks to SnowBe's electronic assets and to reduce risks in alignment with other enterprise risks that are being managed by SnowBe. The program is intended to protect the confidentiality, integrity, and availability of electronic resources and is not intended to prevent, prohibit, or inhibit the sanctioned use of information technology resources as required to meet SnowBe's mission and administrative goals. The program establishes principles for initiating, implementing, maintaining, and improving information security for SnowBe.

Scope of Security Plan

The plan applies to all users, electronic information assets, facilities hosting those assets, applications, systems, network resources, and any other assets, applications, systems, or network resources as designated by SnowBe IT Policy ITP105 Acceptable Use of IT Assets. Affiliated organizations, or any entity, including third parties, using SnowBe information technology resources must operate those assets in conformity with the SnowBe System Security Plan, unless otherwise formally exempted by the President or their designee.

Definitions

SnowBe utilizes various industries' standard definitions compiled and managed by SnowBe Information Technology for all information security and privacy usage. Refer to SnowBe IT Document ITD002, Technical Definitions, for up-to-date list of all standard definitions.

Roles and Responsibilities

All SnowBe employees: Safeguard all data, report occurrences of possible incidents and data breaches to your supervisor or the SnowBe Information Security Officer, and review/comply with SnowBe IT Policies.

Chief Information Officer: Overall owner of SnowBe's IT division and all its assets. Tasked with ensuring all facets of this policy are developed, implemented, enforced, and reviewed.

Chief Information Security Officer: Overall owner of SnowBe's IT Security subdivision and all its assets. Tasked with ensuring all IT assets are secured in accordance with this and all applicable laws, regulations, and business policies.

PCI Compliance Committee: Owner of this policy, ITP103, and responsible for its development, implementation, enforcement, and review.

SnowBe IT Division: Maintain security standards required by PCI DSS, keep current with PCI DSS regulations, and make changes to systems and processes, as appropriate, consult on technical PCI DSS issues, and assist with mandatory annual training sessions.

Third Party Payment Card Processors: Provide confirmation of PCI DSS compliance.

Third Party Vendors: Third party vendors providing hosted services and vendors providing support, whether on site 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 all SnowBe units. All contracts, audits, and risk assessments involving third party vendors will be reviewed and approved by SnowBe IT Division representatives based on their area of responsibility.

Statement of Policies, Standards, Procedures, and Documents

Policies

ITP042 IT Policy Exceptions and Exemptions: This policy provides outlines for the IT exception and exemptions processes for all IT Policies, Standards, and Procedures. Detailed instructions are given for obtaining and revoking exceptions and exemptions.

ITP100 Use of IT Resources: Outlines responsibilities in the user of information technology (IT) resources at SnowBe.

ITP101 Access Control Policy: This Access Control Policy documents requirements of personnel for the appropriate control and management of physical and logical access to, and the use of, state information asset.

ITP102 IT Security: commitment to establishing specific standards, guidelines and procedures affecting key components of its information technology (IT) infrastructure, architecture, and ongoing operations.

IT103 PCI DSS Compliance: 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 the unit and SnowBe.

ITP104 Mobile Device Policy: The purpose of this policy is to define the use of mobile devices when accessing SnowBe's IT Resources.

ITP105 Firmware Updates: This policy documents requirement of personnel for the management of firmware updates to SnowBe assets.

ITP106 SSL/TLS Policy: This policy documents foundational requirements for management of all SnowBe SSL/TLS implementations.

ITP107 Change Control Policy: The purpose of this policy is to ensure that all changes to SnowBe IT Resources minimize any potential negative impact on services and Users.

Procedures

ITSP001 New Account: This standard procedure details the process of creating a new user account for SnowBe IT resources.

ITSP002 Password Management: This standard procedure details the process of managing user passwords.

Standards

ITS001 Password Standard: The purpose of this standard is to establish account management practices for SnowBe Access, the central identity and password manager control system. Management and access control practices are used to ensure security is applied effectively.

Documents

ITD001 IT Exceptions and Exemptions: This document contains all exceptions and exemptions to the IT Security Plan, IT Policies, Standards, and Procedures.

ITD002 Technical Definitions: This document contains applicable standard definitions from various industries compiled and managed by SnowBe Information Technology for all information security and privacy usage.

ITD003 SSL/TLS Implementation List: This document contains all SnowBe's SSL/TLS implementations, both current and past.

Exemptions

Exceptions or exemptions to this plan are reviewed and enacted on a case-by-case basis. For further details on obtaining an exception or exemption from this policy, please refer to SnowBe IT Policy ITP-042, IT Exceptions and Exemptions.

Version History

Version	***Date***	***Description***
1.0	*01/05/2023*	*Initial release*
2.0	*01/15/2023*	*Added Access Control Policies and Document Section*
3.0	*01/20/2023*	*Added Firmware, SSL/TLS, and Change Management policies and New Account procedure*
4.0	*01/28/2023*	*Added Password SOP and Standard; Minor editorial changes*

Citations

ODU IT Security Program

ISU IT Security Plan