SNOWBE ONLINE SECURITY PLAN

Group Members:
Robert Castleberry - Section 02
Josh Hanel - Section 02
Schmyia Terrell - Section 01
Daniel Velez - Section 01
Jeff Whitcomb - Section 01
Danielle Williams - Section 01
Mariluz Williams - Section 01
Version #6 08/29/2024

Table of Contents

Section 1: Introduction

The purpose of this security plan is to improve as well as secure the operations of SnowBe Online and consumer data. To secure operations we must ensure confidentiality, integrity, and data availability. With that aim in mind, SnowBe Online, its employees, and affiliates must adhere to the procedures, policies, and goals laid out by this security plan. SnowBe Online needs to be compliant with local and international regulations where operations take place. This includes, but is not limited to: PCI DSS, SOX, CCPA, GLBA, GDPR, EPrivacy Directive. This plan will provide all necessary information to keep and ensure a compliant, and secure business for its users (employees, affiliates, and consumers).

Section 2: Scope

This plan applies to the entire SnowBe community, including the CEO, Directors, Department Heads, employees, third-party vendors, affiliates, and any other parties with access to SnowBe resources. This will also apply to places of operation, operating systems including mobile devices, and network infrastructure. The scope of this document is limited to the areas where SnowBe Online maintains sole responsibility. If at any point there is any shared responsibility, then those shared responsibilities will be included in this document and outline SnowBe's online responsibility.

Section 3: Definitions

Approval Form
The approval Form is a document used to provide a brief description of the proposed Policy Action and memorialize approval of policies.

Authorized User
An authorized user is any SnowBe employee, contractor, vendor and agent with remote access privileges granted by the Network Administrator.

Change
A Change is defined by an addition, modification, or removal of configuration item that could have an effect on SnowBe operations and which is approved by management, enhances business process changes (fixes) and minimize risk to IT Services. The scope of this definition includes changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

Change Management
Change Management refers to the process used to control the lifecycle of all changes.

Change Proposal
A Change Proposal describes a proposed major Change, like the introduction of a new service or a substantial change to an existing service. The purpose of Change Proposals is to communicate a proposed major Change and assess its risk, impact and feasibility before design activities begin.

Change Record
A Change Record contains all the details of a Change, documenting the lifecycle of a single Change. It is usually created on the basis of a preceding Request For Change.

Cloud Services
A paradigm for enabling on-demand network access to a shared pool of physical and virtual computing resources that support self-service provisioning and management. Division of management responsibilities between the customer and provider vary by service model.

Compliance
Adherence to legal, regulatory, or contractual requirements that dictate how long certain types of data must be retained. This ensures that the organization meets its obligations and avoids penalties or legal action.

Confidential Information
Confidential Information is information protected by statutes, regulations, [Company] policies or contractual language. Information Owners may also designate Information as Confidential. Confidential Information is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a “need-to-know” basis only. Disclosure to parties outside of [Company] must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Configuration Item (CI)
A Configuration item is any component or service that is managed in order to deliver an IT service. These include IT services, hardware, software, process documentation, and service level management.

Containment
The phase in which measures are taken to limit the spread and impact of an incident. Containment is critical for minimizing damage during an incident.

Data Disposal
The secure destruction of data that is no longer required by the organization. This term ensures that data cannot be accessed or reconstructed after disposal.

Data Retention
The practice of storing data for a specific period to meet legal, regulatory, business, or operational requirements. This term outlines how long data should be kept and when it should be securely disposed of.

Department Change
Any change that will only affect one department at SnowBe.

Effective Date
The Effective Date is the date upon which a Policy and/or Procedures will be published, implemented, and take effect.

Emergency Change
An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs) and state regulations.

Implementation Plan
The Implementation Plan is a roadmap for identifying and preparing to address all impacts of the proposed Policy Action.

Incident
An event that disrupts or can disrupt the confidentiality, integrity, or availability of information, systems, or services. This term is central to understanding what triggers the incident response process.

Incident Response
The process of detecting, analyzing, containing, eradicating, recovering from, and learning from incidents. This term encapsulates the entire procedure for managing and mitigating incidents.

Incident Response Team (IRT)
A designated group responsible for responding to security incidents. This team plays a crucial role in executing the incident response process. In this case, the IRT should be composed of: The CISO, the CTO, Compliance Officer, Data Protection Officer, Network Administrator/s, System Administrator/s, and a Technical Consultant.

Information Resource
Any asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can be stored in many forms, including: hardware assets (e.g. workstation, server, laptop) digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including: courier, electronic or verbal communication.

Infrastructure as a Service (IaaS)
On-demand access to cloud-hosted physical and virtual servers, storage, and networking – the backend IT infrastructure for running applications and workloads in the cloud.

Interim Policy
The Interim Policy is a Policy that is approved by the Compliance Officer in accordance with this Policy on an interim basis in situations where a Policy Action must be taken within a period that is too short to permit the completion of the Review and Approval processes.

Legal Hold
A directive to preserve all relevant information when litigation is expected. This overrides normal retention policies, ensuring that data is not altered or deleted until the hold is lifted.

Maintenance Window
A Maintenance Window is a period of time designated in advance by the technical staff, during which

preventive maintenance that could cause disruption of service may be performed.

Network Session
A lasting connection in a network protocol or between a user and a peer, typically a server, usually involving the exchange of many packets between the user's computer and the server.

Non-Privileged Accounts
All Accounts with access to SnowBe's internal network that are not privileged accounts are considered non-privileged. Non-privileged accounts are considered authorized and must abide by all procedures, guidelines and rules outline in this Account Creation Procedure, in the Access Management, and the Account Management policies.

Non-Substantive
Non-Substantive refers to revisions to a Policy and/or Procedures that modify position titles; change department, division, or other entity names; update contact information; correct typographical, grammatical, or citation errors; fix broken hyperlinks; reformat, reorganize, or provide clarifications to improve readability without changing the substance or meaning; or remove or change references to laws, regulations, other policies or materials that have changed or become obsolete.

Normal Change
A Normal Change is a change that does not have a pre-approved SOP and is not classified as an Emergency Change; it follows the full Change Management Process and has a predefined maintenance window.

Organizational Change
Any change that if implemented will affect either multiple SnowBe departments OR SnowBe customers is considered an organizational change.

Platform as a Service (PaaS)
On-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining, and managing applications.

Policy Action
A Policy Action is developing, revising, or discontinuing a Policy and/or Procedures.

Post-Incident Review
A formal review conducted after an incident is resolved to evaluate the effectiveness of the response and identify lessons learned. This term is essential for continuous improvement in incident response efforts.

Privileged Accounts
Privileged accounts are accounts that have access to sensitive and protected resources included but not limited to the CDE(cardholder data environment).

Release
A set of new, changed and/or unchanged Configuration Items that are tested and introduced into IT environments together to implement one or multiple approved Changes.

Remediation Plan
Remediation Plans are actions taken to recover after a failed change into production. These plans are required as part of the Release Management process and clearly defines the steps necessary to restore services to its previous level.

Request for Change Form (RFC)
The Request For Change (RFC) is a formal request for the implementation of a Change. An RFC records the details of a proposed Change and must be submitted to Change Management process by the requestor for every non-Standard Change. The document will provide details of the change for approval and prioritization, and a mechanism for ECCG to govern the Change Management process.

Retention Schedule
A document specifying the retention period for various types of data and records. It details how long data must be retained before being archived or disposed of, based on legal, regulatory, and business needs.

Software as a Service (SaaS)
On-demand access to ready-to-use, cloud-hosted application software.

Standard Change
A Standard Change is a pre-authorized change that is low-risk, predictable in its outcome and repeatable through defined work instructions in a standard operating procedure (SOP).

Virtual Private Network (VPN)
A Virtual Private Network creates a means for private communication between geographically distributed locations. SnowBe Authorized Users shall use the SnowBe VPN for remote access from SnowBe devices to SnowBe resources.

Section 4: Roles & Responsibilities

Authorized Users
Authorized users include anyone with an account authorized by SnowBe to access its internal network. Authorized users are responsible for completing setup for authorized accounts and following the rules of Authorized accounts outlined in the Access Management (AC4) and Account Management(AC-) policies.

Chief Executive Officer (CEO)
Assist in the review and approval of policies and procedures.

Chief Information Security Officer (CISO)
Responsible for the overall security of SnowBe’s Information systems. This includes developing and implementing security policies and procedures. Assist in the review and approval of policies and procedures.

Chief Technological Officer (CTO)
Responsible for SnowBe's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

Compliance Officer
Compliance officers make sure companies and organizations work in full compliance with legal regulations and industry-specific guidelines. They also check internal policies and bylaws. In case of regulatory risks or misconduct, compliance officers address concerns and find solutions to these challenges. Assist in the review and approval of policies and procedures.

Compliance (Change) Managers
A Compliance Manager/Change Manager is the person that is responsible for ensuring that changes within their scope are managed from inception through presentation and into implementation. The scope of a compliance manager is either Organizational focused or Department focused.

Data Protection Officers
Responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of information technology resources and data they own. Assist in the review and approval of policies and procedures.

Department Heads
Assist in the drafting of policies and procedures when necessary.

Departmental Change Control Group (DCCG)
The Departmental Change Control Group is responsible for the oversight of changes to any changes environments that are not organizational changes.

Drafting Committee
An ad hoc committee that should include any heads or managers of affected departments as well as knowledgeable personnel from SnowBe's IT department. Oversee reviewing policy action proposals and drafting initial policies to be reviewed by the Policy Review Committee.

Human Resources Manager
Oversee all aspects of human resources within an organization, including administrative functions, strategic planning, and employee relations. Human Resources Managers are also required to complete initial set-up for all SnowBe employees, contractors, or third-parties that require access to SnowBe's internal network.

Information Technology(IT)
Responsible for configuring the SnowBe VPN in accordance with bet practices.

Network Administrator
Responsible for network configuration, maintenance, monitoring, optimizing, documenting, and reporting. Review and approve remote access request to SnowBe's Network, as well as ensure security of connected systems. Assist in the review and approval of policies and procedures.

Organizational Change Control Group (OCCG)
The Organizational Change Control Group is charged with overseeing the Change Management process for each Change and executing enterprise level change decisions. The Compliance Officer will chair with IT department Head as co-chair with a unanimous decision voting method.

Review and Approval Committee
An ad hoc committee that should include SnowBe's Network Administrator, SnowBe's Chief Information Security officer, SnowBe's Data protection officers, SnowBe's CEO, and one Board member to represent SnowBe's shareholders. Review and submit policies to the Compliance Officer for final review and approval.

Service Owner (SO)
The role that is accountable for the delivery of a specific IT Service. IT managers are the Service Owners for all IT services. Service Owners can delegate decision making for services to leaders within their departments as needed.

Store Managers (U.S & Europe)
Responsible for upholding SnowBe's online guidelines at store locations and holding staff accountable for following guidelines.

Staff and affiliates
Any person who works for or with SnowBe Online is responsible for familiarizing themselves with secure work policies and standards to comply with them.

Sensitive Systems
A sensitive system is any system owned by SnowBe deemed to hold data, resources, or access to data and resources protected by state or federal regulations.

System Administrator
Responsible for the entire lifecycle of hardware and software assets, system Admins manage troubleshooting, licensing and updating.

Technical Consultant
A consultant is an independent contractor, typically an expert in the field, who is not an employee of the Institute and is normally paid as a vendor.

Section 5: Statement of Policies, Standards and Procedures

Policies

AC1 Policy and Procedures – This policy establishes a transparent, consistent, and standardized approach for all policies and procedures to be collaboratively created, revised, discontinued, reviewed, approved, and maintained. This Policy serves to promote awareness, compliance, risk mitigation, and accountability across SnowBe.

AC2 Remote Access - This policy defines requirements for connecting to the SnowBe network from external devices via remote access technology. This policy will define the usage and restrictions for remote access, support, maintenance, and administration mechanisms.

AC3 Access Enforcement - This policy enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC4 Access Management – This policy outlines guidelines for creating, maintaining, and terminating user accounts to ensure the security of SnowBe's systems.

AC5 Separation of Duties - This policy identifies, and documents organization-defined duties of individuals requiring separation and defines system access authorization.

AC6 Least Privilege – This policy ensures that employees are granted only the minimum level of access necessary to perform their job functions, reducing the risk of unauthorized access and potential breaches.

AC7 Unsuccessful Logon Attempts – This policy establishes controls for managing repeated failed login attempts to enhance security and prevent unauthorized access.

AC8 System Use Notification – This policy requires clear and visible notifications for users before they access the company's systems, informing them of authorized use and monitoring practices.

AC9 Wireless Access – This policy outlines guidelines for securing wireless networks, including strong encryption, access point security and regular monitoring to protect unauthorized access.

AC10 Concurrent Session Control – This policy regulates the number of simultaneous user sessions allowed per account to enhance security and prevent unauthorized access.

AC11 Device Lock - This policy is established to ensure that all devices used within the organization are secured to prevent unauthorized access and protect sensitive information, including customer data and personally identifiable information (PII).

AC12 Session Termination – The policy Session termination addresses the requirements before the termination of user-initiated logical sessions.

AC13 Publicly Accessible Content – This policy addresses systems that are controlled by SnowBe and accessible to the public, typically without identification or authentication.

AC14 Use of External Systems – This policy establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and / or maintaining external information systems, allowing authorized individuals to access the information system from external information systems.

AC15 Reference Monitor - This policy ensures that all access to information systems is continuously monitored and enforced to protect sensitive data from unauthorized access

SP1 Data Retention – This policy dictates how long customer information and internal sensitive data should be kept and when it should be securely disposed of.

SP2 Incident Response - This policy sets up the procedures to follow in case of a security breach, including identification, containment, and recovery steps.

SP3 Encryption- This policy is to establish, at a senior management level, the Business and Compliance expectations that the organization needs to meet. The policy serves as a starting point to define the sustainable Encryption that the Company needs to meet.

SP4 Data Classification-The Data Classification Policy identifies and helps protect sensitive and confidential data with framework of rules, processes and procedures for each class. OBJ

SP5 Physical Security Policy - The Physical Security Policy is to establish the rules, procedures, and guidelines for granting, control, monitoring, and removal of physical access to SnowBe's Information Resource facilities in order to protect physical resources from accidental damage or intentional attacks.

SP6 Identity Access Management Policy - The purpose of the SnowBe IAM Policy is to establish the requirements necessary to ensure that access to and use of SnowBe Information Resources is managed in accordance with business requirements, information security requirements, and other SnowBe policies and procedures.

SP7 Remote Work Policy - This policy outlines SnowBe's guidelines for employees who work from a location other than our offices. We want to ensure that both employees and our company will benefit from these arrangements.

SP8 Segregation of Duty Policy – This policy is responsible for performing their duties in accordance with proper Internal Controls as established by management. Segregation of duties is critical because it ensures separation of different functions and defines authority and responsibility over transactions. Segregation of duties is also a key Internal Control; it reduces the risk of errors and inappropriate actions.

SP9 Firewall Policy - This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to SnowBe's network and information systems.

SP10 Password Policy - The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

SP11 Acceptable Use Policy – This sets rules related to SnowBe's IT security policies. These include rules around accessing restricted information; changing access data such as passwords, opening questionable email attachments, using public Wi-Fi services, and using company approved authentication procedures.

SP12 Vendor Management Policy – This policy is to help SnowBe's organization conduct third-party information security risk management. All vendors, suppliers, partners, and other third parties accessing SnowBe's data and systems. Helps prescribe how SnowBe can identify and deal with potentially risky vendors.

SP13 Disaster Recovery Policy – This policy is a plan that will outline how SnowBe Company response in the unexpected events that disrupt business needs.

SP14 Network Security Policy- This Policy is a formal document that outlines the guidelines, procedures and principles for maintaining, monitoring, and enforcing security on a computer Network. This would be beneficial to SnowBe Company since it is a well traffic company. Protecting user information is at the upmost important.

SP15 Cloud Security Policy – This policy sets the guidelines for procedures and controls to protect data, applications, and infrastructure associated with SnowBe cloud computing. This policy aims to mitigate risk, ensure data integrity and maintain confidentiality of information stored on SnowBe cloud servers.

SP16 Mobile Device Policy – This policy sets the guidelines and rules designed to protect SnowBe's data and resources when accessed through a mobile device. This policy aims to secure sensitive information, prevent unauthorized access, and manage risk associated with mobile devices used to access SnowBe's data.

SP17 Change Control Management - This policy's objective is to ensure that standardized methods and procedures are used to enable beneficial changes while ensuring efficient and prompt handling of all changes to services. This policy aims to minimize the disruption of services, reduce back-out activities, and ensure clear communication across SnowBe, its employees, and when applicable its customers.

PCI Policy 1- This policy document provides information to ensure SnowBe complies with PCI DSS in an effort to protect cardholder data. This document represents SnowBe's procedures to prevent loss or disclosure of customer information including credit card numbers.

Standards and Procedures

SOP1 Create New Account – This procedure standardizes the steps to create a new user account in order to access SnowBe's internal network.

SOP2 Password Standard - This standard identifies the minimum password requirements needed to protect SnowBe's data and systems. Passwords are used on SnowBe devices and systems to facilitate authentication, i.e. helping ensure that the person is who they say they are. The security of SnowBe 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 employees, or attacks directed at SnowBe customers from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of private data such as private cardholder data and/or private employee data.

SOP3 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 creation of strong passwords, the protection of those passwords, and the frequency of change.

Section 6: Exceptions/Exemptions

Any exceptions or exemptions to the security policies, standards, and procedures outlined in this plan must adhere to the following criteria;

- All requests must be documented in detail, including the specific reasons for the exception, potential risks involved, and any compensating controls implemented to mitigate those risks.
- Approval must be obtained from the Network Administrator and the relevant department manager, with final oversight and approval by the Director or Manager of Information Technology.
- All exceptions will be granted on a case-by-case basis, documented in a centralized exception tracking system, and reviewed at least quarterly by the Incident Response Team (IRT) to assess any changes in risk or compliance requirements.
- Exceptions that pose significant risks or affect regulatory compliance must be reported to the Compliance Officer for additional review.

Section 7: Version History Table

Version	Date	Description
1	08/08/2024	Introduction, scope, roles and responsibilities, and exceptions/exemptions added.
2	08/12/2024	Fixed formatting errors, and grammatical errors. Definitions were added, Roles and Responsibilities updated, as well as Policies.
3	8/19/2024	Fixed formatting errors. Added Access Control Policies and updated roles and responsibilities as well as definitions where necessary. Edited exemptions/exceptions clause for clarity.
4	08/26/2024	Attempted to address formatting concerns. Added change Control Management Policy and New Account Procedure. Added Cryptography and Encryption Controls to the policy.
5	08/26/2024	Fixed formatting to address spacing when formatted into a PDF.
6	09/01/2024	Added SOP 2 Password standard and SOP 3 Password Procedure

Citations

Sample Security Plan
https://www.compliancewire.com/EduFlexCourses/Courses/C_769_4247/Assets/lang_1/jobaids/sample_security_plan.pdf

Michigan Technological University Information Security Plan
https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

Oregon Cybersecurity Plan
https://www.oregon.gov/oem/Documents/Oregon-Cybersecurity-Plan.pdf

Alice Lloyd College Security Plan
https://www.alc.edu/wp-content/uploads/2022/06/Security-Plan-2022_.pdf

University of Tennessee Security Exceptions and Exemptions
https://policy.tennessee.edu/procedure/gp-001-02-security-exceptions-and-exemptions-to-its-standards-practices-controls/

Drata – What is a Retention Policy?
https://drata.com/blog/data-retention-policy

TechTarget – What is a Retention Policy?
https://www.techtarget.com/searchdatabackup/definition/data-retention-policy

Center for Internet Security – Incident Response Policy Template
https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

Hyperproof – Data Classfication Policy
https://hyperproof.io/resource/data-classification-policy/#:~:text=A%20data%20classification%20policy%20identifies,and%20procedures%20for%20each%20class.

Resourcers for Employers – Remote Work Policy Template
https://resources.workable.com/remote-work-policy

University of Missouri – Segregation of Duties
https://www.umsystem.edu/ums/policies/finance/segregation

NICCS – Glossary of Common Cybersecurity Words and Phrases

https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#explore-terms-a-

glossary-of-common-cybersecurity-words-and-phrases

National Cybersecurity Society - Remote Access Policy Template
https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Remote-Access-Policy-Template-FINAL.pdf

University of Oklahoma - https://itsupport.ou.edu/TDClient/30/Unified/KB/ArticleDet?ID=3049

Support Center - https://supportcenter.ct.edu/Service/CCC_policies/RemoteAccessPolicy.pdf

Anne Arundel Community College - https://www.aacc.edu/policies/policy-on-development-of-policy-and-procedures/

Drata Change Managment- https://help.drata.com/en/articles/8364890-change-management-policy-guidance

Louisiana Department of Administration -
https://www.doa.la.gov/media/lhibcody/ots_change_management_policy.pdf

FRSecure policy template - https://frsecure.com/change-management-policy-template/

Data Apex SOP - https://www.dataapex.com/documentation/Content/regulated-environment/040-sop/040.000-sop/040.000-sop-setup-user-account.htm

Michigan technology University Information Technology - https://www.mtu.edu/it/security/policies-procedures-guidelines/password-standards.pdf