SNOWBE ONLINE SECURITY PLAN

James Chapman

Version # 5.0.0
Date 06/01/25

Table of Contents

Section 1: Introduction

The SnowBe Security Plan aims to establish the framework for protecting the company's information and assets. This plan will include the necessary policies, procedures, and controls to keep SnowBe's data safe from unauthorized users. This security plan outlines multiple security controls that will ensure company integrity, protect customer data, and ensure compliance requirements are met to maintain a successful business operation. Since SnowBe Online processes, stores, and transmits cardholder data, SnowBe Online must comply with PCI DSS (Payment Card Industry Data Security Standard). This includes our European operations, which must also adhere to PSD2 (Payment Services Directive). With our customers in mind, we will provide a safe and secure shopping platform that ensures a smooth process with every session.
The following security measures will take place to ensure SnowBe Online operates on Confidentiality, Integrity, and Availability.
- Data security and data risk assessment
- Access control and User management to protect against unauthorized access to sensitive data
- Security controls and updates are managed for all firmware and software
- Risk assessment on all servers and networks
- Device protection for all networked devices

Section 2: Scope

This security plan will apply to all employees, contractors, and third-party vendors who have access to SnowBe Online's information systems. We have designed this security plan to oversee defined security measures to protect SnowBe Online including our operations, network infrastructure, network hardware and software, our VPN, data servers, and all connected devices including all organization internal and external assets connected to SnowBe Online's network perimeter.

Section 3: Definitions

Access Controls – A technique used to regulate access to resources within a network environment.
CIA (Confidentiality, Integrity and Availability) – A method used to protect the confidentiality of data, enforce integrity assurance, and ensure availability to resources by managing risks within a network infrastructure.
Exploit – A program designed to take advantage of a vulnerability in a computer system.
Identity Management tool (IAM) – A tool used to authenticate a user, and then grants access based on least privilege rules.
Information System Owners (ISOs) – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Payment Services Directive (PDS2) – The Payment Services Directive (PSD2) is a European Union (EU) law that regulates payment services and payment service providers.
PCI DSS (Payment Card Industry Data Security Standard) – A set of rules and guidelines designed to protect Payment Card Processing.
Risk Assessment – A process used for identifying potential exploits.
Third Party Vendors – In relation to SnowBe Online, Third-Party Vendors are any entity that provides outside services such as software, transportation, lodging, or accommodations to guests

beyond the scope of SnowBe's services.
Vulnerability – A potential access point to gain unauthorized access.

Section 4: Roles & Responsibilities

Chief Information Security Officer (CISO) – One who is responsible for developing, implementing, and maintaining the security polices as well as the procedures.
Department Managers – A member of this department will be responsible for making sure their teams comply with all security policies as well as report any security incidents.
Employees – They are expected to comply with the security policies, as well as attend training. They must also report any suspicious activities.
Information System Owners (ISOs) – Official(s) responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
IT Manager – Will monitor and approve and implement the security controls. They will also conduct audits on a regular basis in addition to providing security training.
SnowBe Personnel – This includes all contractors, subcontractors, hired employees, c-level executives, seasonal workers, and all other individuals working under the SnowBe company letterhead.
Technical Analyst – One who will investigate the root cause of an incident that occurs. They will also collect digital evidence.
Third-Party Vendor – Are responsible for following all guidelines and requirements stated in partnership contracts. They must also abide by all data security policies and procedures stated in the partnership contract.

Section 5: Statement of Policies, Standards and Procedures

Policies

AC 1 Policies and Procedures – The purpose of this policy is to manage risks as they relate to Access Control. The policy statements describe controls, that when implemented by supporting standards and procedures, are designed to move the associated risks to an acceptable level.

CM 1 Change Control Management – Addresses how changes in relation to controls that are implemented in organizations and systems are handled. These controls help manage any risks, asset protection, and any business objectives are achieved securely. This is critical for maintaining system confidentiality and integrity.

SP 1 Web Application Security – Accounts for the largest portion of attack vectors outside of malware. It is vital that any SnowBe web application be assessed for vulnerabilities and that any vulnerabilities be remediated before production deployment.

AC 2 Account Management – Account management allows SnowBe to differentiate the level of privilege given to certain groups of personnel.

SP 2 Remote Access – Remote access to SnowBe network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are

at a significantly lower security posture than our corporate network.

AC 3 Access Enforcement – Will enforce approved authorizations for logical access to system resources and information.

SP 3 Virtual Private Network – The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the SnowBe Online corporate network.

AC 4 Information Flow Enforcement – This can be seen as the other side to access control. Here we control what types of data are allowed to reach certain destinations, thus ensuring data flow is secure, and always tracked.

SP 4 Server Malware Protection – This responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications.

AC 5 Separation of Duties and Least Privilege – This policy defines that all personnel must only receive access to the lowest possible level of privilege needed to conduct their duties. It also establishes procedures for the separation of duties within the information technology environment.

SP 5 Removable Media – Minimize the risk of loss or exposure of sensitive information maintained by SnowBe and to reduce the risk of acquiring malware infections on computers operated by SnowBe.

SP 6 Social Engineering Awareness – To make employees of SnowBe aware fraudulent social attacks occur and educate them on the proper response in each case.

AC 7 Unsuccessful Logon Attempts – Enforces account lockout after a defined number of consecutive invalid attempts.

SP 7 PCI DSS – Protects payment card data and customer information as 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 SnowBe Online brand.

AC 8 System Use Notification and Previous Logon Notification – This policy ensures that the end user must acknowledge the organization’s system use guidelines before access is granted. This will also provide the user with the logon information from their last logon.

SP 8 Internet Usage – A set of guidelines that explain to the employees of SnowBe what is deemed acceptable for using the company's internet.

SP 9 Risk Assessment – This will involve how SnowBe will assess as well as manage any risks that might come across various areas of its activities.

SP 10 Email Access – This policy is designed to create guidelines and requirements for secure email access across the organization, keeping private communications out of the hands of unauthorized users, data secure, and in accordance with all applicable regulations. The policy is

designed to standardize email security while streamlining business communication.

AC 11 Device Lock and Session Termination – All devices owned and operated by SnowBe must be programmed to require re-authentication after certain periods of inactivity. This is designed to ensure that authorized personnel who leave their station momentarily, don't jeopardize sensitive data to public exposure. When long periods of inactivity, or other triggering events, occur, it's paramount to require personnel to re-authenticate into their sessions. This reduces the likelihood of the operator having changed from an authorized to unauthorized individual during the duration of a session.

SP 11 Mobile Device Encryption – This policy will enforce mandatory encryption of organizational data on mobile devices. This policy was designed to protect confidential data when the device is lost or stolen, comply with data protection laws and keep business data access on mobile devices secure.

SP 12 Cloud Security – The purpose of this policy is to establish guidelines and standards for securing SnowBe Online's cloud environments. This policy aims to protect sensitive data, prevent unauthorized access, and ensure the availability of cloud-based services in alignment with the company's strategic goals and compliance requirements.

SP 13 Third-Party Security – The purpose of this policy is to establish standards and procedures for evaluating, monitoring, and managing third-party vendors to ensure they comply with SnowBe Online's security and privacy requirements. This policy aims to mitigate risks posed by third-party access to company systems, data, and operations.

SP 14 Data Loss Prevention – The purpose of the Data Loss Prevention Policy is to keep any confidential or private information safe from being lost or stolen. This would help SnowBe in keeping their information safe from any attackers or from being lost in general.

SP 15 Physical Security and Access Control – The purpose of the Physical Security and Access Control Policy is to create guidelines to keep safe any of SnowBe's physical assets or information from any unauthorized access, destruction or theft.

AC 18 Wireless Access – This policy establishes guidelines for secure wireless network access within SnowBe's Infrastructure. All wireless access points must be configured with enterprise-level encryption protocols, requiring secure authentication methods, and be regularly monitored for unauthorized access attempts. All guest wireless networks must be segregated from the main corporate networks, and all wireless traffic must be encrypted using current industry standards. Regular wireless network audits must be performed to eliminate any rogue access points found.

SP-01 Patch Management Policy - The Patch Management Policy establishes a standardized approach for identifying, testing, and deploying security patches and updates across all SnowBe Online information systems. Its purpose is to reduce vulnerabilities, protect company assets, and ensure compliance with regulatory requirements by maintaining the confidentiality, integrity, and availability (CIA) of SnowBe's technology infrastructure.

SP-02 Security Maturity Policy - The Security Maturity Policy outlines the use of an industry-recognized security maturity model to assess, benchmark, and continuously improve SnowBe Online's security posture. It ensures that all critical domains are regularly evaluated, documented,

and advanced through defined maturity levels, fostering a culture of ongoing security enhancement and risk reduction.

SP-03 System Development Life Cycle (SDLC) Policy - The System Development Life Cycle (SDLC) Policy defines secure development practices for all SnowBe Online systems, including AWS-hosted, WordPress, and on-premise environments. It mandates structured planning, threat modeling, secure coding, rigorous testing, and documentation at every phase to ensure regulatory compliance and the protection of sensitive data throughout the system lifecycle.

Standards and Procedures

PR 1 New Account Creation Procedure – This procedure shows the expected steps for account creation within an organization. This allows for accounts to be created securely, with the correct compliance and access controls. This helps maintain security and accountability within the organization.

ST 1 Password Standard – The purpose of this Standard is to establish the minimum requirements for passwords used to access SnowBe Online Information Systems to reduce the risk of Unauthorized Access to SnowBe Online technology resources and data.

PR 2 Password Procedure – 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

The mission of SnowBe is to create, through the use of Policy, Standard, and Procedure, a secure environment for SnowBe Online employees, customers, and all affiliates. We understand that in the process of policy implementation, exceptions may be requested.

Personnel of SnowBe may request an exemption for some of the following reasons: Unforeseen Operational Circumstances, Testing New Programs, Policy Misalignment, or Impacted Workflow. If SnowBe Personnel wishes to apply for an exception to a particular IT policy, the following procedures must be followed:

1. The requestor must submit a written request to the SnowBe Online IT Manager. The requestor must provide sufficient detail within the written request, for the SnowBe Online IT Manager to adequately consider the request. For example, the written request must include the following: a detailed, extensive written reason why the request is being made.

2. The SnowBe Online IT Manager will review the exception request and identify the potential risk(s) involved in granting the exception within 5 business days.

3. The SnowBe Online IT Manager will schedule a meeting with the requestor. At that meeting, the SnowBe Online IT Manager will review the request with the requestor and if the risk is low, the SnowBe Online IT Manager may grant the exception. If the risk is not low, the decision on whether to grant the request must be made by the IT Director of SnowBe Online.

4. If the exception request is granted, it is assumed that the requestor agrees to implement whatever risk mitigation protocols are recommended and associated with the exception, and failure to do so may subject the requestor to disciplinary sanctions. If the exception request is denied, the requestor must adhere to the policy at issue.

5. The SnowBe Online IT Manager has the authority to set time limits on exceptions. If a time limit exists, the SnowBe Online IT Manager will notify the requestor thirty (30) days prior to the expiration of the exception for either renewal, alternate solutions, or discontinuation of the exception. The SnowBe Online IT Manager has the authority to revisit a previously granted exception at any time, should the risk level of an exception rise due to changed circumstances.

Section 7: Version History Table

Version	Date	Description
1.0	01/08/25	Security Plan Working Draft
1.1	01/13/25	Added Policies
2.0	01/20/25	Added Access Controls
3.0	01/26/25	Revised Exemption/Exception and Scope
4.0	02/02/25	Revised Exemption/Exception and Scope, Updated CM 1 from Configuration Management to Change Control Management Added Standard ST 1 and PR 1
5.0	06/01/25	Added SP-01, SP-02, SP-03

Citations

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf - reference for Purpose, Scope, and Definitions

https://www.ferc.gov/sites/default/files/2020-04/security-plan-example.pdf - Research on Purpose.

https://www.techtarget.com/searchsecurity/definition/incident-response-team - Research and reference materials for possible roles and responsibilities.

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf - Web page used to acquire PCI DSS Security Standards PDF.

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf - PCI DSS Security Standards PDF.

https://centricconsulting.com/blog/security-exceptions-the-ultimate-weakness-to-a-secure-environment/ - Used to research Exceptions and wording references.

https://security.virginia.edu/exceptions?form=MG0AV3 - used to research Definitions, Exceptions and Purpose.

https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/Information_Security_Plan_0.pdf - Used as a reference to formulate scope and introduction.

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf - Used as a reference to formulate scope and introduction.

https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/data-and-system-security-policy.html - Used as reference material for Purpose, and Scope.

https://www.oxy.edu/policy-directory/information-security-plan - Used to Research Information Security Plans and industry wording as reference.

https://security.ucop.edu/policies/it-policies.html - Used to reference policy wording and glossary for definitions.

https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/NetworkSecurityPolicy_UPC_0.pdf - Used to formulate scope.

https://policy.tennessee.edu/procedure/gp-001-02-security-exceptions-and-exemptions-to-its-standards-practices-controls/ - Used to formulate Exemptions/Exceptions.