# SnowBe Online
# Security Plan (SP)

September 24, 2022
Version Number: 4.0

# Table of Contents

# 1. Introduction

This Security Plan constitutes the "Standard Operating Procedures" relating to physical, cyber, and procedural security for all SnowBe Online. It contains a comprehensive overview of the SnowBe Online's security program, and in some sections, makes reference to other relevant plans and procedures. Security personnel, operators, and selected SnowBe Online personnel shall be familiar with the information and procedures associated with this Security Plan.

# 2. Scope of Security Plan

SnowBe Online is responsible for protecting the confidentiality, integrity, and availability of the company's information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of SnowBe Online, violate individual privacy rights, and possibly constitute a criminal act. It is the collective responsibility of all users to ensure they are familiar with and adhere to SnowBe Online policies, including privacy, acceptable use of information technology resources, and other facilities and properties policies.

This plan applies to any use of the SnowBe Online's computing or network resources as defined in the Acceptable Use of Information Technology Resources, and the other facilities and property policies. Additional standards and procedures may govern specific data or computer systems or networks provided or operated by Third-party service providers. This plan applies to all university personnel and entities and is to be read by all university technical support staff and information asset owners.

# 3. Definitions

**Access Control**
The process of granting or denying specific requests to:

- Obtain and use information and related information processing services; and
- Enter specific physical facilities (ex.: Office buildings, Vendor establishments).

**Affiliate**
An Affiliate is an entity, be it a person or organization, that is officially attached or connected to an organization, e.g., contractors, vendors, interns, temporary staffing, volunteers.

**Authorized user**
An individual who has approved access to an information asset to perform job responsibilities.

**Cable Modem**
Cable companies provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

**Challenge Handshake Authentication Protocol (CHAP)**
CHAP is an authentication method that uses a one-way hashing function.

**Cloud Computing Application**
Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Common examples of cloud computing applications are Dropbox, Facebook, Google Drive, Salesforce, and Box.com.

**Confidential Information**
Confidential Information is information protected by statutes, regulations, SnowBe Online 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 SnowBe Online must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Information include:
- Customer data shared and/or collected during the course of a consulting engagement
- Financial information, including credit card and account numbers
- Social Security Numbers
- Personnel and/or payroll records
- Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
- Any Information belonging to an SnowBe Online customer that may contain personally identifiable information
- Patent information

**Coordinator**
SnowBe Online official who has oversight responsibility for the regulation/standard. Regulation monitors stay abreast of updates to their respective regulations, ensure policies are up to date and notify CNS about changes.

**Credit Card Data**
Full magnetic strip or the PAN (Primary Account Number) plus any of the following:
- Cardholder name
- Expiration date
- Service Code

**Data Custodian**
Any SnowBe Online official, who, based on his/her position, is a fiduciary owner of specific SnowBe Online information assets. For instance, the Payroll Director (or designee) is the SnowBe Online Data Custodian for SnowBe Online's Unemployment Compensation Information Assets.

**Data Link Connection Identifier (DLCI)**
DLCI is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.

**Demilitarized Zone (DMZ)**
A SnowBe Online host or network segment inserted as a "neutral zone" between the organization's private network and the Internet.

**Dial-in Modem**
A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus, the name "modem" for modulator/demodulator.

**Digital Subscriber Line (DSL)**
DSL is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

**Enforce password history**
Describes the best practices, location, values, policy management, and security considerations for the Enforce password history security policy setting.

**Frame Relay**
A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

**Incident**
An incident can have one or more of the following definitions:
**A.** Violation of an explicit or implied SnowBe Online security policy
**B.** Attempts to gain unauthorized access to a SnowBe Online Information Resource
**C.** Denial of service to a SnowBe Online Information Resource
**D.** Unauthorized use of SnowBe Online Information Resources
**E.** Unauthorized modification of SnowBe Online information
**F.** Loss of SnowBe Online Confidential or Protected information

**Information Assets**
The full spectrum of all SnowBe Online's information technology products, including business applications, system software, development tools, utilities, appliances, and so forth.

**Information Resource**
An 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. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.

**Integrated Services Digital Network (ISDN)**
There are two flavors of ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

**Internal Information**
Internal Information is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Information is information that is restricted to personnel designated by SnowBe Online, who have a legitimate business purpose for accessing such Information.

Examples of Internal Information include:
- Employment Information
- Business partner information where no more restrictive confidentiality agreement exists
- Internal directories and organization charts
- Planning documents

**Maximum password age**
Describes the best practices, location, values, policy management, and security considerations for the Maximum password age security policy setting.

**Merchant Account**
A relationship between SnowBe Online and a bank in order to accept credit card transactions. The merchant account is tied to a general ledger account to distribute funds appropriately to the organization (owner) for which the account was set up.

**Minimum password age**
Describes the best practices, location, values, policy management, and security considerations for the Minimum password age security policy setting.

**Minimum password length**
Describes the best practices, location, values, policy management, and security considerations for the Minimum password length security policy setting.

**Mobile Device**
Computing devices that are intended to be easily moved and/or carried for the convenience of the user, and to enable computing tasks without respect to location. Mobile devices include, but are not necessarily limited to mobile phones, smartphones, tablets, and laptops.

**PAN**
Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

**Password must meet complexity requirements**
Describes the best practices, location, values, and security considerations for the Password must meet complexity requirements security policy setting.

**PCI DSS**
Payment Card Industry Data Security Standard

**PCI Security Standards Council**
The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

**Penetration Test**
A highly manual process that simulates a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment.

**Personal Devices**
Include the following categories:

- Portable cartridge/disk-based, removable storage media (ex.: floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards or drives that contain nonvolatile memory);
- Portable computing and communication devices with information storage capability (ex.: notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices); and
- Any other mobile computing device small enough to be easily carried by an individual, able to wirelessly transmit or receive information, and having local, nonremovable data storage and a self-contained power source.

**Personally-owned**
Systems and devices that were not purchased and are not owned by SnowBe Online.

**Public Information**
Public Information is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public Information, while subject to SnowBe Online disclosure rules, is available to all SnowBe Online employees and all individuals or entities external to the corporation.

Examples of Public Information include:

- Publicly posted press releases
- Publicly available marketing materials
- Publicly posted job announcements

**Principle of Least Privilege**
A security principle whereby users are assigned the minimum access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.

**Privileged User**
A user who is granted rights that go beyond those of a typical business user to manage and maintain IT systems. Usually, these rights include administrative access to networks and devices and are separate from users' administrative access to their own workstations.

**Public/Private Key**
In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.

**Removable media**
Portable devices that can be used to copy, save, store, and/or move Information from one system to another. Removable media comes in various forms that include, but are not limited to, USB drives, flash drives, read/write CDs and DVDs, memory cards, external hard drives, and mobile phone storage.

**Self-Assessment**
The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

**Separation of Duties**
A security principle that divides critical functions among staff members to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud (ex.: no user should be given enough privileges to misuse the system on their own).

**Split Tunneling**
Split Tunneling is a computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections.

**Store passwords using reversible encryption**
Describes the best practices, location, values, and security considerations for the Store passwords using reversible encryption security policy setting.

**Virtual Private Network (VPN)**
VPN is a method employing encryption to provide secure access to a remote computer over the Internet.

**Vulnerability Scan**
A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.

# 4. Roles and Responsibilities

**Businesses, Departments, and Other Units**
Businesses, departments, and other units are responsible for securing any information they create, manage, or store, and for any information they acquire or access from other SnowBe Online's systems (e.g., personnel records, business information). This responsibility includes completing periodic risk assessments, developing and implementing appropriate security practices, and complying with all aspects of this policy.

When credit card processing is part of the department business process, perform an annual PCI DSS self-assessment (SAQ) and submit the report to the SnowBe Online Treasurer's Office for approval.

Any SnowBe Online department accepting payment card data must designate an individual(s) who will have primary authority and responsibility for payment acceptance.

All SnowBe Online departments, users accepting payment cards will complete PCI training upon hire and annually thereafter. See UTECH Policy III-1e Controls – Restricted Information: Case Information Security Requirements for Restricted Information.

Any SnowBe Online department accepting payment cards will utilize only the SnowBe Online Treasurer's office approved equipment to process card payments.

**Chief Information Officer (CIO)**
The CIO has overall responsibility for the security of the SnowBe Online's information technologies. Implementation of security policies is delegated throughout the company to various services; to departments, and other units; and to individual users of SnowBe Online's IT resources.

**Chief Information Security Officer (CISO)**
The CISO is a senior-level executive responsible for developing and implementing SnowBe Online's security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats. The CISO will also investigate any reported violations of this plan, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the plan or any of its other policies.

**Critical Incident Readiness Team (CIRT)**
CIRT is responsible for providing for rapid, systematic, and coordinated early intervention in critical incidents. CIRT works with the President and other university leaders to address critical incidents.

**Data Custodian**
The data custodian is the individual or entity (including outsourced services) in possession or control of data and is responsible for safeguarding the data according to the policies and procedures established by the associated data steward. The appropriate level of protection is based on the SnowBe Online Data Classification policy and the Minimum Security Standards for Protected Data.

**Data Protection Officer (DPO)**
The DPO is responsible for ensuring that SnowBe Online is compliant with GDPR. The DPO should:

- Provide advice and guidance to SnowBe Online and its employees on the requirements of the GDPR
- Monitor the SnowBe Online's compliance
- Be consulted and provide advice during Data Protection Impact Assessments
- Be the point of contact for data subjects
- DPOs should also take responsibility for carrying out data audits and oversee the implementation of compliance tools

**Data Steward**
This role is represented by an executive officer. The data steward has policy-level and planning responsibilities for data owned by SnowBe Online. Data stewards, as a group, are responsible for recommending policies, establishing procedures and guidelines for company-wide data administration activities. Data stewards may delegate the implementation of SnowBe Online policies, standards, and guidelines to data custodians.

**Director Endpoint Protection and Identity and Access Management**
This role is responsible for ensuring various aspects of SnowBe Online's Endpoint Protection and Identity and Access management:

- Ensuring that SnowBe Online's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the organization from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- Ensuring that SnowBe Online's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible
- Ensuring that SnowBe Online's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible.

**Director of Facilities Management**
The Director of Facilities Management will ensure that support/training and resources are available to the Security Team to implement the Security Policy, including assembling and maintaining a suitably qualified security team.

**Director of Information Security (DIS)**
The DIS is responsible for ensuring various aspects of Iowa State's cyber and information security:

- Ensuring that SnowBe Online's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the organization from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- Ensuring that SnowBe Online's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.
- Ensuring that SnowBe Online's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible.
- Ensuring that SnowBe Online's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities.

**Director of Physical Security**
The Director of Physical Security is responsible for all strategic aspects of security across SnowBe Online's properties.

**Individuals Using Personally-Owned Computers and Other Network Devices**
All individuals who use personally-owned systems to access university resources are responsible for the security of their personally-owned computers or other network devices and are subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by the IT Services for SnowBe Online computing and network facilities.
- All other laws, regulations, or policies directed at the individual user.

**Head of Security**
The Head of Security will be responsible for the development of strategic security, drafting the SnowBe Online's Physical Security Policy, and will take the lead role in its implementation and will propose amendments to the Physical Security Policy that may be necessary in the future.

**IT Security and Policies Team**
The IT Security and Policies Team is responsible for ensuring the security of SnowBe Online's provided IT services. The security and policy team must make sure that all intellectual property and proprietary information are protected. This role is responsible for taking all necessary preventions to ensure the security of the services provided by SnowBe Online.

**Management and Responsibilities**
It is essential that adequate resources are made available for managing the risk arising from security related issues within SnowBe Online. It is important that all personnel involved in implementing this policy are competent, trained, and aware of their responsibilities.

**Other Registered Entities**
Any entity that is a registered user and connected to the SnowBe Online's network is responsible for the security of its computers and network devices and is subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by IT Services for SnowBe Online's computing and network facilities.
- All other laws, regulations, or policies directed at SnowBe Online and its individual users.

**Security Operations Manager**
The Security Operations Manager will manage the day-to-day implementation of the Security Policy and monitor its continued effectiveness.

**Security Staff**
Security staff will perform regular vulnerability scanning of network devices where PCI payments are scanned, submitting risk reports to the SnowBe Online's Treasurer's Office. Support software for data loss prevention service for users to audit IT systems for presence of PCI data. The Security Staff will carry out duties as defined in the SnowBe Online Operational Procedures Manual. See appendix I: Security Operational Procedures.

**Security Team Leaders**
Security Team Leaders will be responsible for the day-to-day organization and supervision of security officers as defined in the operational procedures. See Appendix I: Security Operational Procedures

**Senior Responsible Owner (SRO)**
SROs are responsible for ensuring that the requirements of this plan are implemented within any program, projects, systems or services for which they are responsible, as designated by the CISO.

- The SRO is responsible for ensuring that a robust checking regime is in place and complied with to ensure that legitimate user access is not abused.
- The SRO may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and associated checking regime.
- Any non-compliance with this policy must be supported by a documented and evidence based risk decision accepted by the SRO.

**Staff**
All staff must be knowledgeable of and adhere to SnowBe Online's Security Plan

**Third Party Vendors**
Third party vendors providing hosted services and vendors providing support, whether on SnowBe Online's premises or from a remote location, are subject to SnowBe Online 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 businesses, departments, and other units. All contracts, audits and risk assessments involving third party vendors will be reviewed and approved by SnowBe Online's Data Steward based on their area of responsibility.

# 5. Statement of Policies, Standards, and Procedures

## *5A. Policies*

**SP01 - Access Control Policy**
This policy defines the policy and procedures for implementing and maintaining appropriate access controls for SnowBe Online information assets.

**SP02 - Backup Policy**
This policy outlines the IT Department's backup policy for the computer systems in use by SnowBe Online and follows industry standards for providing Disaster Recovery capabilities for SnowBe Online's computer systems.

**SP03 - Change Control Management Policy**
This policy:

- Establishes the rules for the creation, evaluation, implementation, and tracking of changes made to SnowBe Online's Information Resources.
- Ensures that standardized methods and procedures are used to enable beneficial changes, while ensuring efficient and prompt handling of all changes to services provided by SnowBe Online's IT Department.
- Minimizes the disruption of services, reduce back-out activities, and ensure clear communication across SnowBe Online, the IT Department, and its customers.

**SP04 - Computer Passwords Policy**
This policy identifies standards and parameters for SnowBe Online's systems login credentials and passwords for all individuals who are responsible for safeguarding access to SnowBe Online's systems.

**SP05 - Physical Security Policy**
This policy establishes the rules for the granting, control, monitoring, and removal of physical access to SnowBe Online's Information Resource facilities.

**SP06 - PCI Compliance Policy**
This policy provides guidance about the importance of protecting SnowBe Online's 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 Online.

**SP07 - Remote Access Policy**
This policy defines standards for connecting to SnowBe Online's network from any end user device (ex., PC, Laptop, 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 college confidential data, intellectual property, damage to public image, and damage to critical Connecticut College internal systems.

**SP08 - Software, Firmware, and Information Integrity Policy**
This policy ensure that SnowBe Online's IT resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

## *5B. Standards and Procedures*

**STAN01 - New Password Creation Standards**
These standards safeguard SnowBe Online's systems access login identification ("SBOID") and password credentials.

**PROC01 - New Network Account Creation Procedures**
These procedures document the creation process for new SnowBe Online network accounts.

**PROC02 - New Password Creation Procedures**
These procedures document the creation process for passwords to access SnowBe Online network accounts.

# 6. Exemptions

Exemption from certain policy provisions may be sought by following the SnowBe Online Exemption Process.

# 7. Exceptions

Personnel found to have violated this plan or any of its policies may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this plan or any of its policies may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

# 8. Evaluation and Revision of the Security Plan

This Security Plan will be evaluated and adjusted to reflect changing circumstances, including changes in the SnowBe Online's business practices, operations, or arrangements, or as a result of testing and monitoring the safeguards.

# 9. Version History Table

| Date | Version | Description |
|---|---|---|
| 09/06/2022 | 1.0 | Security Plan week 1 |
| 09/11/2022 | 1.1 | Security Plan week 1 Corrections |
| 09/14/2022 | 2.0 | Security Plan week 2 |
| 09/20/2022 | 3.0 | Security Plan week 3 |
| 09/24/2022 | 4.0 | Security Plan week 4 |

# 10. References

SP01 - Access Control Policy
SP02 - Backup Policy
SP03 - Change Control Management Policy
SP04 - Computer Passwords Policy
SP05 - Physical Security Policy
SP06 - PCI Compliance Policy
SP07 - Remote Access Policy
SP08 - System and Information Integrity Policy

STAN01 - New Password Creation Standards

PROC01 - New Network Account Creation Procedures
PROC02 - New Password Creation Procedures