SNOWBE ONLINE

Policy # SP-03

Security Awareness Training Policy

Daphnie Bruno

Policy # SP-03 - Version 1.0

October 30, 2024

Table of Contents

Purpose

The Security Awareness and Training Policy establishes the requirements to assist Information Technology (IT) system managers, administrators, and users of SnowBe Online systems and data the steps to ensure that SnowBe Online systems and data are appropriately safeguarded. Our executives, staff, vice presidents, interns, managers, senior managers, board members, contractors and business partners are the frontline to protecting SnowBe Online's data assets and this policy will assist at providing consistent guidance and overall approach to security awareness.

Scope

SnowBe Online provides Security Awareness Training for all executives, staff, vice presidents, interns, managers, senior managers, board members, contractors and business partners prior to assessing SnowBe Online data and information technology resources and annually. The training will address roles, responsibilities, management commitment, proper disposal of data storage media, coordination among organizational entities and compliance. (Note: Special focus is given to sensitive system and data concerns.)

Definitions

Acceptable Use Policy - A document that outlines the rules and guidelines for using an organization's IT systems and resources.

Access Controls - Mechanisms for restricting and managing access to systems, including creating and changing passwords and maintaining their confidentiality.

Data Owner - An individual responsible for the management and integrity of specific data within an organization.

Encryption - The process of converting information or data into a code to prevent unauthorized access.

Information Security Officer - A role responsible for overseeing and implementing an organization's security awareness and training program.

Intellectual Property Rights - Legal rights that protect creations of the mind, including software licensing and copyright issues.

Least Privilege - The principle of providing users with the minimum levels of access or permissions needed to perform their job functions.

Malicious Code - Software designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing - A cybercrime technique using fraudulent emails or websites to trick individuals into revealing sensitive information.

Remote Access Policies - Guidelines governing how users can securely connect to an organization's network

from outside locations**.**

Role-Based Training - Specialized security training tailored to specific job roles and responsibilities within an organization.

Security Awareness Training - Educational programs designed to inform users about information security risks and best practices

Security Incident - An event that potentially compromises the confidentiality, integrity, or availability of an information system or data

Sensitive Data - Information that requires protection from unauthorized access or disclosure.

Separation of Duties - A principle that divides tasks and privileges among different individuals to prevent fraud and errors

Social Engineering - Manipulative tactics used to deceive people into divulging confidential information or performing actions that compromise security.

System Administrator - An individual responsible for maintaining and operating computer systems and networks

System Owner - A person accountable for the overall management and security of a specific information system

Roles & Responsibilities

The IT Security Program roles and responsibilities are assigned to individuals and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as, the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

SnowBe Online Employees
Faculty, Faculty Administrators, Staff, Contractors, Vendors, and Business Partners who use SnowBe Online IT systems will be required to:

- Complete an annual online Security Awareness Training course every twelve (12) months.
- All newly hired employees are required to complete the Security Awareness Training course within the first 30 days from date of hire or prior to receiving access to the SnowBe Online IT systems and data.
- Additional Security Awareness Training may be required by all employees at other intervals when IT infrastructure environment changes.
- Read the "Acceptable Use Policy" and electronically sign the IT Acceptable Use Standards and User Acknowledgement Agreement" which acknowledges that they are fully aware of security best practices, their roles in protecting the SnowBe Online information technology systems and data. Access to SnowBe Online computer technology will not be granted without this agreement.

Supervisors, Managers, and Directors are required to:

- Ensure each employee under his/her supervision has attended and completed the Security Awareness Training and should include the training as a part of the employee's annual performance evaluation.
- Maintain a copy of each employee's Security Awareness Training certificate in the department's personnel file.
- Managers will ensure that SnowBe Online employees, interns, managers, senior managers, board members, contractors and business partners who manage, administer, operate, or design IT systems, receive additional role-based information security training as deemed appropriate and that is commensurate with their level of expertise, role and responsibilities.

System Owners

- Facilitate and participate in practical cybersecurity training exercises on an ad hoc basis that simulate cyber-attacks and threats for situational and enterprise readiness.
- Complete annual role-based training (or more frequent intervals based upon enterprise needs) and maintain records of training.

System Administrators

- Facilitate and participate in practical cybersecurity training exercises on an ad hoc basis that simulate cyber-attacks and threats for situational and enterprise readiness.
- Complete annual role-based training (or more frequent intervals based upon enterprise needs) and maintain records of training.

Data Owner

- Complete annual role-based training (or more frequent intervals based upon enterprise needs) and maintain records of training.

Information Security Officer

- Aligns the SnowBe Online Security Awareness Program with the Commonwealth's SEC 501-09.1 Standard and industry best practice.
- Oversees SnowBe Online Security Awareness and Training program, including development, implementation and testing.
- Coordinates, monitors and tracks the completion of the Security Awareness Training for all SnowBe Online executives, staff, vice presidents, interns, managers, senior managers, board members, contractors and business partners and report incomplete training to the respective senior executive, manager or accountable person.
- Develops the role-based training and maintains records of training for entire program.

Policy

1. This Security Awareness and Training policy applies to all SnowBe Online employees (permanent, temporary, contractual, faculty, and administrators) who are responsible for the development, coordination, and execution and use of SnowBe Online information technology resources to conduct SnowBe Online business and to transmit sensitive data in the performance of their jobs.
2. It is the policy of SnowBe Online that the Technology Services department will implement information security awareness and training best practices. At a minimum, these practices include the following components:
    - Implement, maintain, and provide on-going information technology Security Awareness Training using various training delivery techniques in awareness sessions, use email distribution for security awareness communications, and publish a security web site to promote and reinforce good security practices, SnowBe Online policies and procedures, and employee responsibilities.
    - Establish accountability and monitor compliance by implementing an automated tracking system to capture key information regarding program activity (i.e. courses, certificates, attendance, etc.).
3. All SnowBe Online employees (permanent, temporary, contractual, faculty, and administrators) who use SnowBe Online information technology resources to conduct SnowBe Online business and to transmit sensitive data in the performance of their jobs must take security awareness training prior to using SnowBe Online systems, when required by information system changes; and annually thereafter.
4. In an effort to educate SnowBe Online system users in understanding their responsibility in safeguarding systems and data, security awareness training will include the following concepts:
    - The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
    - The concept of separation of duties;
    - Prevention and detection of information security incidents, including those caused by malicious code;
    - Proper disposal of data storage media;
    - Proper use of encryption;
    - Access controls, including creating and changing passwords and the need to keep them confidential;
    - Agency acceptable use policies;
    - Agency Remote Access policies;
    - Intellectual property rights, including software licensing and copyright issues;
    - Responsibility for the security of COV data;
    - Phishing;
    - Social engineering;
    - Least privilege.
5. Role specific training will be provided to the following specialized users (System Owners, Data Owners, and Security Administrators). Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. This training will also provide the training necessary for individuals to

carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to the SnowBe Online.

6. To ensure compliance with the annual security awareness training, training will be documented and monitored for individual information system security training activities including basic security awareness training and specific information security training (i.e. role-based training); and
7. Training records to support training activities will be retained for period as defined by the SnowBe Online records retention policy.

Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will last for a specified duration, at most 90 days, unless additional justification is provided.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Enforcement

Violations of this IT Security Plan will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

<Template Policy> – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner:
DATE

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	30-Oct-24	Daphnie Bruno		First Draft

Citations

State of Oregon Enterprise Information Services Information Security Plan

https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-statewide-information-security-program-plan.pdf

Information Security Plan from Washington and Lee University

https://my.wlu.edu/its/about-its/information-security-plan

Virginia State University Policies Manual

https://www.vsu.edu/files/docs/policies/6000/6530-security-awareness-training.pdf