SNOWBE ONLINE Policy #0002
Security Training and Awareness Policy

Sean Redding

Security Training and Awareness

Policy – V.10 10/05/2025

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 3

POLICY 3

EXCEPTIONS/EXEMPTIONS 4

ENFORCEMENT 4

VERSION HISTORY TABLE 4

CITATIONS 6

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

Purpose

The Security Awareness and Training Policy establishes the requirements to assist Information Technology (IT) system managers, administrators, and users of Snowbe Online's systems and data, the steps to ensure that university systems and data are appropriately safeguarded. Our faculty, Staff and students are the frontline to protecting the university's data assets, and this policy will assist in providing consistent guidance and an overall approach to security awareness.

Scope

SnowBe provides Security Awareness Training for all university faculty, staff, deans, vice presidents, interns, managers, senior managers, board members, contractors, and business partners before assessing SnowBe's data and information technology resources, and annually. The training will address roles, responsibilities, management commitment, and proper disposal of data storage media, coordination among organizational entities, and compliance.

- Special focus must be given to sensitive systems and data concerns.

Definitions

BYOD Policy: Bring Your Own Device Policy, an essential policy to manage and secure endpoints

CISO: The senior-level information security employee with the title of Chief Information Security Officer.

Endpoint - An endpoint is any physical device that can be connected to a network, including computers, laptops, mobile phones, tablets, and servers.

Information Owner: The individual(s) or Unit with operational authority for specified University Information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This individual or Unit is responsible for making risk tolerance decisions related to such Information on behalf of the University and is organizationally responsible for any loss associated with a realized information security risk scenario.

Company Data: Snowbe Information and related resources, such as equipment, devices, software, and other information technology.

Information System: A major application or general support system for storing, processing, or transmitting Snowbe's Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

Information System Owner: The individual(s) or Unit responsible for the overall procurement, development, integration, modification, operation, and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of Snowbe Online and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

Roles & Responsibilities

Chief Information Security Officer (CISO):

- Holds accountability for orchestrating an effective security awareness and training program.
- Ensures all employees are informed and equipped to safeguard both the organization's and our community members' digital assets.

Information Technology (IT) Department:

- Crafting and sustaining an extensive collection of information security guidelines, which encompasses this policy.
- Collaborates with other departments to facilitate proper awareness and training sessions. These sessions are aimed at enlightening staff about their duties, as outlined in various policies, regulations, contracts, and more.

Managers:

- Ensure teams under their purview actively participate in security training and awareness initiatives.
- Ensure that all employees under their charge are up to date with their required training.

All employees, contractors, and volunteers:

- Personally responsible for completing all mandated security awareness training modules.

[BYOD users] - Information Owners and Information System Owners

Information Owners and Information System Owners are also responsible for implementing processes and procedures designed to ensure compliance with the minimum standards

Policy

This Security Awareness and Training policy applies to all SnowBe's employees (permanent, temporary, contractual, faculty, and administrators) who are responsible for the development, coordination, execution, and use of the company's information technology resources to conduct business and to transmit sensitive data in the performance of their jobs.

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 ongoing information technology Security Awareness Training using various training delivery techniques in awareness sessions, Use email distribution for security awareness communications, and publish a security website to promote and reinforce good security practices, SnowBe's 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.).

Exceptions/Exemptions

Requests for an exception, must be submitted in writing to consult with the IT Director or IT Manager.
The request must be detailed with information, including:
· Length of time
· Policy or standard
· Reason
And the Exception Request form must be signed by:
· CIO
· Information Security Officer
· CEO
· Commissioner
Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.
If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.
The CISO, the information security officer representing, and the commissioner must maintain constant communication during the exception. If approved, the CISO's office will send the letter of approval to the requester, along with the details. In the event of denial, a letter of explanation will be sent to the requester, stating the reason for the CISO's denial and providing an explanation.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

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

Version #	Implementation Date	Document Owner	Approved By	Description
V 1.0	10/05/2025	Sean Redding		Initial draft of Security Training and Awareness Policy

Citations

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

https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint/

https://policy.arizona.edu/information-technology/information-security-awareness-training-policy

https://fullsailedu-my.sharepoint.com/:w:/g/personal/spredding_student_fullsail_edu/EXjlypAOvOJlni_SA2h3v5IBEWufCIh0Cgisl8bZV06LmA?e=SQOKYp