SNOWBE ONLINE
Policy 5.1.2 SECURITY AWARENESS AND TRAINING

Adam Duckworth

VERSION 1.0 June 6, 2023

Table of Contents

Purpose

(Please note that this has been adapted from Connecticut College Information Services Security Awareness Training Policy)

The purpose of this policy is to ensure that all SnowBe employees affiliates with access to company data, are taught Information Security Awareness in order to gain an understanding of the importance of securing said data. SnowBe Online seeks to establish a culture that ensures that all company data is secure.

Scope

(Please note that this has been adapted from Connecticut College Information Services Security Awareness Training Policy)

This policy applies to all SnowBe employees and identified affiliates.

Definitions

(Please note that this has been adapted from Connecticut College Information Services Security Awareness Training Policy)

Security Awareness Training - a formal process for educating employees about the internet and computer security. A good security awareness program should educate employees about company policies and procedures for working with information technology (IT).

Contractor - someone officially attached or connected to SnowBe Online who is not an employee.

Personally Identifiable Information (PII) - any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Data Owner - a person responsible for the management and fitness of data elements (also known as critical data elements) - both the content and metadata.

Policy

(Please note that this has been adapted from Connecticut College Information Services Security Awareness Training Policy)

Educating employees and contractors at all levels on the safe and responsible use and handling of information is necessary. It is the obligation of SnowBe Online's staff to protect company-owned electronic devices containing company and customer data. This data exists for the purpose of SnowBe business. To facilitate appropriate information security practices, management requires specific training based on the classification level of data you have access to.

Full-time employees are required to attend security awareness training upon employment with the company. Employees have 30 days to complete the training progra, or they will be deemed non-compliant with this policy. Employees with access to PII must take security awareness training on a yearly basis. All third-party contractors who have access to PII information must undergo security awareness training before they can access the company data.

The security awareness training program is subject to yearly review and enhancement based on changes to the information security environment.

Exceptions/Exemptions

(Please note: this has been adapted from The University of Tennessee System)

Requests for exceptions from SnowBe security controls, standards, or practices must be submitted in writing to the IT Department. At a minimum, each request shall have the following information completed by the requestor, or the request will not proceed:

- Contact information on the requestor and authorized signer
- The standard, practice, or controls from which an exception is desired
- Request type (i.e. Exception, Exemption)
- Explanation of the Request
- Business Justification/Reason

The IT Department conducts a risk assessment on the request.

- If needed, the IT Department will conduct a review of the assessment.

The IT Department documents the results of the risk assessment and will then accept or reject the request.

All requests that are granted must be reviewed and/or renewed annually.

Enforcement

(Please note: this has been adapted from the SANS Acceptable Use Policy)
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Version History Table

Version #	Change/ Implementation date	Document Owner	Approved By	Description
1.0	June 6, 2023	SnowBe Online	Adam Duckworth	Initial Draft

Citations

Acceptable use policy - assets.contentstack.io. (n.d.). https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt207beda4b7c14d22/636f1a30e3836b0c88e8f0a8/Acceptable_Use_Policy.pdf

GP-001.02 – security exceptions and exemptions to its standards practices & controls. UT System Policies. (2022, June 23). https://policy.tennessee.edu/procedure/gp-001-02-security-exceptions-and-exemptions-to-its-standards-practices-controls/

Information security awareness policy. Connecticut College. (n.d.). https://www.conncoll.edu/information-services/policies/information-security-awareness-policy/