Sam Houston State University
A Member of The Texas State University System
Information Technology (IT)

Security Awareness and Training Policy: IT-13

PURPOSE:

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This will be accomplished with a combination of general computer security awareness training and targeted product-specific training. The philosophy of protection and specific security instructions need to be taught to and re-enforced with technology users. The security awareness and training information needs to be continuously upgraded and reinforced.

The purpose of the Security Awareness and Training Policy is to describe the requirements that ensure each user of SHSU information resources receives adequate training on technology security concepts and issues. Additionally, state law requires that institutions of higher education provide an ongoing information security awareness education program for all users of state-owned information resources (Texas Administrative Code (TAC) §202).

SCOPE:

The SHSU Security Awareness and Training Policy applies to all SHSU employees and contractors.

POLICY STATEMENT:

1. All employees and contractors must complete the SHSU Cybersecurity Awareness Training within 30 days of initially being granted access to SHSU information resources, or per request of the data owner or supervisor.

2. Annually, all employees must complete the SHSU Security Awareness training and pass the associated examination.

3. Annually, all employees must sign a non-disclosure agreement per IT-16 Non-Disclosure Agreement Policy stating they have read and understand SHSU requirements regarding IT policies and procedures.

4. IT must prepare, maintain, and distribute an Information Security User Guide that concisely describes SHSU information security policies and procedures.

5. IT must develop and maintain a communication plan that will communicate security awareness to the SHSU user community.

6. Per Texas Government Code Title 10, Subtitle B, Chapter 2054, Subchapter A,

Section 076, all SHSU employees who administer and/or maintain information resources require yearly cybersecurity continuing education. This cybersecurity continuing education should be related to the employee's duties and is in addition to the annual cybersecurity awareness training. The number of hours per fiscal year varies depending on an employee's duties and are listed in the following table:

All Information Resources Employees	1 hour per fiscal year
Employees with administrative privileges or responsibilities for Information Resources	3 hours per fiscal year
Information Security or Cybersecurity staff	6 hours per fiscal year

Employee managers or supervisors are responsible for identifying employees who perform administrative, security, governance, or compliance activities on information resources and ensure that the required number of continuing education hours are met for each employee per the Texas DIR Information Resources Employees Continuing Education Guidelines for Cybersecurity.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, May 2, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, May, 2023
Next Review: May, 2024