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

IT Policy Compliance: IT-00

PURPOSE:

The purpose of this policy is to ensure information resources and services promote the basic mission of the University. Sam Houston State University (SHSU) established information resources and services for the use and benefit in its conduct of academic, business, and other official operations.

This document provides direction and support for the SHSU Information Security Program and Information Technology Policies. The collection of policies represents the basis of the SHSU Information Security Program and, on the aggregate, is subject to and is intended to comply with Texas State University System (TSUS) Rule III, Para. 19 and its associated guidelines.

This policy promotes the following goals:

- To ensure the confidentiality, integrity, and availability of SHSU information resources and services;
- To ensure that use of SHSU information resources and services is consistent with the principles and values that governs SHSU as a whole;
- To ensure that information resources and services are used for their intended purposes; and
- To ensure all individuals granted access privileges to SHSU information resources and services have a clear understanding of what is expected during use and the consequences of violating SHSU policies.

SCOPE:

This policy applies equally to all individuals granted access privileges to any SHSU information resources and services.

POLICY STATEMENT:

1. Pursuant to the TSUS Rules and Regulations Chapter III §19.2, TSUS IT Policies found at https://gato-docs.its.txst.edu/jcr:9df1a102-7773-4503-8ce5-6c1cddafae8b/TSUS%20IT%20Policy%20-%202022.pdf are adopted as official SHSU policy. TSUS IT Policies are authoritative and establish the minimum requirements for SHSU. Additional SHSU IT and information security policies, standards, procedures, and guidelines are enhancements and adaptations specific to SHSU.

2. Users have a responsibility to protect and respect SHSU's information resources and services, and understand the regulations and policies that apply to their appropriate use.

3. SHSU information technology resources and services may be limited or regulated by SHSU to fulfill the primary mission of the university. Usage may be constrained as required to assure adequate capacity, optimal performance, and appropriate security of those resources and services.

A User is defined as anyone who accesses any SHSU information resources and services.

4. Users implicitly consent to university monitoring for any lawful purpose, including but not limited to, evidence of possible criminal activity, violations of law, contract, copyright, or patent infringement, and/or violation of any university or TSUS policy, rule, or regulation.

5. Users must adhere to all SHSU and TSUS information technology policies.

6. Each state institution of higher education shall submit to the department a biennial Information Security plan, in accordance with §2054.133, Texas Government Code and Texas Administrative Code (TAC) 202.73(b)(3).

7. The Information Security Program must be reviewed and approved at least annually by the head of the institution. TAC 202.70(7).

NON-CONSENSUAL ACCESS:

1. SHSU will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that SHSU will not seek access to their electronic messages or documents without their prior consent except where necessary to:

    - Satisfy the requirements of the Texas Public Information Act, or other statutes, laws or regulations;
    - Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
    - Protect the integrity of SHSU's information technology resources, and the rights and other property of SHSU;
    - Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations; or
    - Protect the rights of individuals working in collaborative situations where information and files are shared.

2. SHSU cannot absolutely guarantee the privacy or confidentiality of electronic documents. Consequently, persons that use these state-owned resources, or any personally owned device that may be connected to an SHSU resource, have no expectation of or right to privacy in their use of these resources and devices.

To appropriately preserve the privacy of electronic documents and allow authorized individuals to perform their assigned duties, specific university staff and law enforcement will sign an SHSU Non-Consensual Access to Electronic Information Resources Request Form annually and submit the form to the Office of the Information Resources Manager (IRM). At the beginning of each fiscal year, non-consensual access designations will be resubmitted, reviewed, and approved or denied by the IRM and University President.

VIOLATIONS:

1. Failure to adhere to the provisions of the information technology policies may result in:

    - suspension or loss of access to institutional information resources and services
    - appropriate disciplinary action under existing procedures applicable to students, faculty, and staff, and
    - civil or criminal prosecution

2. Potential violations will be investigated in a manner consistent with applicable laws and regulations, SHSU policies, standards, guidelines, and practices.

EXCEPTIONS TO POLICY:

Exceptions are granted on a case-by-case basis and must be reviewed by the Information Security Officer and approved by the University designated IRM. The required Policy Exception Form and procedures can be found at http://www.shsu.edu/intranet/policies/forms/. The IRM will mandate the documentation and additional administrative approvals required for consideration of each policy exception request.

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 TSUS Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.03
Approved by: President's Cabinet, April 11, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, April, 2023
Next Review: April, 2024