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

Policy Compliance: IT-00

PURPOSE

The purpose of this policy is to ensure an information technology infrastructure that promotes the basic mission of the university. SHSU's information services network has been established for the use and benefit of SHSU in the conduct of its academic, business, and other operations. This document provides direction and support for the SHSU Information Security Program and the Division of Information Technology Services (IT@Sam) Policies.

This framework of IT security policies collectively represent the basis of the institutional Information Security program and on the aggregate whole meet the objectives as articulated by TSUS Rule III, Para. 19 and it associated guidelines.

This policy promotes the following goals:

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

SCOPE

This program applies equally to all individuals granted access privileges to any Sam Houston State University (SHSU) information technology resources.

POLICY STATEMENT

Information technology resources play an integral part in the fulfillment of the primary mission of the university. Users of SHSU's information technology resources have a responsibility to protect and respect those resources, and are responsible for knowing the regulations and policies that apply to appropriate use of the university's information technology resources.

Users must understand and expect that SHSU information technology resources may be limited or regulated by SHSU, if needed, 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.

Anyone using SHSU's information resources expressly consents to university monitoring of the network at any time and for any purpose, including but not necessarily limited to, evidence of possible criminal activity, violations of law, contract, copyright or patent infringement, and/or violation of any university or Texas State University System policy, rule, or regulation.

SHSU information security policies can be found on the SHSU website at: http://www.shsu.edu/intranet/policies/information_technology_policies/index.html

The Information Security User Guide which contains a summary of user related policies can be found at: http://www.shsu.edu/~ucs_www/documents/Information_Security_User_Guide.pdf

The Information Security Program, which contains the framework that will ensure the appropriate safeguards are applied to SHSU information systems, can be found at: http://www.shsu.edu/intranet/policies/information_technology_policies/documents/SHSU_Info_Sec_Program_ver_2012_08_29.pdf

A review of the institution of higher education's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s). TAC 202.71(e)

NON-CONSENSUAL ACCESS

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 right to privacy in their use of these resources and devices. However, 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.

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 requests will be resubmitted, reviewed, and approved or denied by the IRM.

Individuals may request non-consensual access to specific data by initiating the Non-Consensual Access to Electronic Information Resources Request Form, obtaining the approval of their organizational head, and submitting the form to the Office of the Information Resources Manager (IRM). If the request appears compliant with university policy, the IRM or designee will coordinate with the Information Security Officer (ISO) as necessary to satisfy the request.