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 represents the basis of the institutional Information Security program and on the aggregate whole meet the objectives as articulated by the Texas Administrative Code (TAC) §202), National Institute of Standards and Technology (NIST)800.53, and The 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/dotAsset/c4bd0a47-e173-40ce-bdc6-71fa9d9d1cbd.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/Info_Sec_Program.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)

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 information and enable personnel to perform their official duties, SHSU will formally designation and document personnel will NCA to electronic information. Prior to the start of each fiscal year, the President and IRM will update the NCA Annual Designation form to reflect the personnel identified. The most recent form will supersede any previous form, effective the date of the final signature. IT is the responsibility of the IRM to ensure the form is updated in timely manner when personnel move to a role that no-longer requires NCA or when new personnel are to be added. It is the IRM's responsibility to notify individuals of their authorization and associated

responsibilities. Non-Consensual Access Annual Designation for Electronic Information Resources.

VIOLATIONS

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

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

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

EXCEPTIONS TO POLICY

Exceptions are granted on a case-by-case basis and must be reviewed 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 Texas State University Systems Rules and Regulations, Policy Guideline TSUS IT.02.01, Information Security Policy. The primary applicable references are listed below.

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Administrative Code, Title 5, Subtitle A, Chapter 552 (TAC 202)
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)
- Computer Software Rental Amendments Act of 1990
- The Texas State University System Rules and Regulations

- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets

DEFINITIONS:

Information Technology Resources: All university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Information Resources Manager (IRM): Officer responsible to the State of Texas to manage SHSU information technology resources.

Information Security Officer (ISO): Officer designated to administer the university Information Security Program.

National Institute of Standards and Technology (NIST)800.53: Security and Privacy Controls Catalog for Federal Information systems and Organizations.

Non-Consensual Access: The university shall permit the examination of electronic communication records without the consent of the holder when required by law, when there is a reason to believe that there are violations of university policy, compelling circumstances, or under time-dependent or critical operation circumstances.

System Administrator: Individual(s) who are responsible for running/operating systems on a day-to-day basis.

Reviewed by: Mark C. Adams, VP for Information Technology, May 31, 2013
Approved by: President's Cabinet, September 16, 2013
Reviewed and Approved by: Mark Adams, VP for Information Technology, September 1, 2016
Next Review: November 1, 2018