Sam Houston State University

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM

Information Security & Compliance

SHSU Information Security User Guide

Contents

Sam Houston State University

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM

Information Security & Compliance

Section 1: General Information

1. Introduction

This user guide was written to provide an easy reference for policies associated with the SHSU Information Security Program and Information Security Policies that pertain to employee use of information technology resources. These guidelines summarize acceptable practices to educate individuals on the basic responsibilities needed to begin utilizing information technology resources.

The purpose of this *Information Security Guide* is to describe the requirements that ensure each person has the knowledge to protect SHSU information technology resources, protect themselves and comply with applicable laws. All individuals are accountable for their actions relating to information technology resources and these resources are to be used for intended purposes as defined by SHSU policies and in compliance with applicable laws.

As changes to the user guide are made, they will be published, and replacement pages or sections will be accessible.

2. Overview

Information technology resources are strategic assets (procedures, software, data, equipment and facilities used by SHSU) of the State of Texas, and it is mandatory that SHSU manage these resources as valuable State resources. Measures will be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to assure the availability, integrity, utility, authenticity and confidentiality of information.

The SHSU Information Security Program and associated IT security policies are based on the published Texas Administrative Code, Information Security Standards 1 (TAC § 202), NIST Special Publication 800-53, Security and Privacy Controls (NIST SP 800-53),The Texas State University System (TSUS) Policy Guidelines for information technology security (Chapter 19 and Appendices A-2 through A5) and the state and federal laws and regulations listed in IT-00 Policy Compliance.

This guide contains a summary of user information and responsibilities derived from the IT security policies. For ease of inquiry, each section indicates which policy covers that topic.

Policy location:
https://www.shsu.edu/intranet/policies/information_technology_policies/

3. Applicability

This guide applies equally to all individuals granted access privileges to any SHSU information technology resource. This guide applies to all equipment that is owned or leased by SHSU or connected to the SHSU network. The IT Security Policies apply to those that otherwise create, generate, communicate, store, process, use, and rely on information resources of the SHSU.

4. User Responsibilities

1. **All individuals are accountable for their actions relating to information technology resources.** Users of information resources shall use university resources only for defined purposes and comply with established controls.

   Compliance with SHSU published policies and standards is mandatory. Your responsibility is to adequately secure information technology resources from unauthorized access, data manipulation, disclosure, and theft of protected and confidential information.

2. **You are responsible for knowing the regulations and policies of the university that apply to appropriate use.** Users of these services and facilities have access to valuable university resources, to sensitive data, and to internal and external networks.

3. **You are responsible for exercising good judgment in the use of the university's technological and information resources**.

   Just because an action is technically possible does not mean that it is appropriate to perform that action. Consequently, it is important to behave in a responsible, ethical, and legal manner.

4. **It is your responsibility to attend the Security Awareness Training and to familiarize yourself with the SHSU IT policies** available online at:

   https://www.shsu.edu/intranet/policies/information_technology_policies/

5. **All users must sign the SHSU Non-Disclosure Agreement (NDA)** acknowledging they have read and understand SHSU requirements regarding computer security policies and procedures. (IT-16) This signed non-disclosure agreement becomes permanent record and will be renewed annually.

5. Enforcement

In accordance with IT-00, “Policy Compliance”, violation of University policy may result in disciplinary action which may include termination of employment for employees and temporaries; a termination of employment relations in the

case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Sam Houston State University Information Resources access privileges, civil, and criminal prosecution.

Any violations of state or federal law regarding these policies shall be reported to appropriate Law Enforcement Agency.

6. Obtaining a Policy Exception

Exceptions are granted on a case-by-case basis and must be reviewed and approved by the University designated Information Resources Manager (IRM). The IRM will mandate the documentation and additional administrative approvals required for consideration of each policy exception request.

Section 2: User Security Practices and Safeguards

1. User Accounts (IT-01)

1. You will automatically be assigned a computer account, or username, with SHSU that you will use for any computers and/or systems you log in to. This account is unique and is to be used by you only.
2. Never share your username or password with anyone (including family, friends, co-workers, and supervisors).
3. You are responsible for what is accessed, downloaded, or created with your computer account, regardless of intent. A non-authorized person can cause loss of information confidentiality, integrity and availability that may result in liability, loss of trust, or embarrassment to SHSU.

2. Account Passwords (IT-02)

You must create a strong password and protect it (If you think someone has your password, the password must be changed immediately):

1. Passwords must have a minimum length of fifteen (15) characters. It is strongly recommended that passwords contain a mix of upper case, lower case, and numeric characters or special characters (!@#%^&*+=?/~’;:,<>|\).
2. Passwords must not be easy to guess, for instance, your social security number, your birth date, your nickname, obscenities, etc.
3. Users will be reminded to change passwords at least once every four (4) years.
4. Passwords must be encrypted when stored and never posted on monitors, under keyboards, on sticky notes, etc.

5. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.

3. Acceptable Use (IT-03)

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities, and all pertinent license and contractual agreements.

Acceptable Use of SHSU information technology resources are outlined in detail in IT-03 Acceptable Use Policy, as well as IT-11 Data Backup, IT-12 Network Use Policy, IT-13 Technology Security Training Policy, IT-19 Authorized Software, IT-20 Electronic Communication Policy, IT-24 Computer Virus (Malicious Code), and IT-26 Personal Computing Policy.

All messages, files and documents located on university information technology resources (to include any personal documents) are owned by SHSU, may be subject to Open Records requests, and may be accessed by authorized SHSU IT employees at any time without knowledge of the information resources' user or owner.

Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. Incidental use is permissible as long as it does not violate policy and/or exceed departmental guidelines. If you are uncertain, you should consult your supervisor.

3.1 Personal use guidelines (IT-03)

a. Personal use must not result in direct costs to SHSU.

b. Personal use must not interfere with the normal performance of an employee's work duties. (Excessive use that exceeds incidental is determined by your supervisor.)

c. Users must not use the SHSU information technology resources for private financial gain or personal benefit. (E.g., you may not run a private business on any SHSU information technology resources.)

d. Users must not use SHSU information technology resources for political gain.

e. Users must not use information technology resources to threaten or harass others.

f. Users must not intentionally access, create, store or transmit illegal material.

g. Users must not violate copyright laws by distributing/downloading protected works.

h. Users must not send or forward chain letters.

i. If you access the Internet from a university-owned computer at your home, you must adhere to all the same policies that apply to use from within SHSU facilities.

j. Do not allow non-SHSU users, even family members, to access your SHSU computer systems.

k. Users must not attach a network device (e.g., a wireless access point) to the university network without IT approval. (IT-12)

3.2 Information Integrity (IT-03)

Users must not interfere with or alter the integrity of SHSU information technology resources by:

a. Impersonating other individuals in communication;

b. Attempting to capture or crack passwords or encryption;

c. Unauthorized access, destruction, or alteration of data or programs belonging to other users;

d. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.

3.3 Internet use (IT-03)

a. Sensitive or confidential SHSU material transmitted over external networks shall be encrypted.

b. User activity on SHSU information technology resources is subject to monitoring and review.

c. SHSU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.4 Electronic Communication (IT-20)

a. Do not send, forward, or request to receive confidential or protected SHSU information through or to non-SHSU E-mail accounts.

b. Confidential data must be protected at all times from unauthorized disclosure. Encryption is an acceptable method of data protection.

3.5 Portable Computing (IT-26)

The users of portable computing devices or media used to store, transmit or process protected or confidential data are expected to take all appropriate measures and precautions to prevent the loss, theft, damage and/or unauthorized use and shall include the following:

a. All reasonable precautions to prevent data compromise should be taken when using portable computing devices (e.g., shield screen from passive viewing, password protected screen saver).

b. Ensure the device is shut down or secured when not in use (e.g., password protect devices offering such capabilities).

c. Physically safeguard the devices. Keep portable computing devices within view or securely stored at all times. Unattended portable computing devices must be physically secure (e.g., locked in an office, desk drawer or filing cabinet; in an automobile, secure in a non-visible location).

d. Use encryption to safeguard all storage media, (e.g., hard drives, USB flash drives, flash memory cards).

e. Do not allow unauthorized persons to access SHSU portable computing devices or media. You are responsible for any misuse of the information by persons to whom you have given access.

f. Promptly notify IT if any portable computing device or media has been lost or stolen.

3.6 Technology Security Training (IT-13)

a. All employees and contractors must complete the Texas DIR certified security awareness training within 30 days of being granted access to any SHSU information technology resources and each year thereafter.

b. All employees whose duties include those which are categorized as belonging to Information Resources Employees as defined by Texas DIR, must complete the appropriate level of cybersecurity continuing education each fiscal year.

3.7 Malware (Malicious Code) Protection (IT-24)

a. All workstations and laptops must use IT approved anti-malware protection software and configurations.

b. The settings for the malware protection software must not be altered in a manner that will reduce the frequency of updates, bypass or disable the software.

c. Malware that are not automatically cleared by the malware protection software are security incidents and must be reported to IT by visiting https://www.shsu.edu/report-it, by calling (936) 294- 1950, or by emailing servicedesk@shsu.edu.

3.8 Data Backup (IT-11)

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

a. Any data used in an information technology resource system must be kept confidential and secure by the user.

b. All departments should store data on network storage (e.g. S and T drives) rather than local storage (e.g. PC or Mac hard drives). Local storage is not backed up by IT and may not be able to be recovered.

c. SHSU IT will backup data at regular intervals and protect that data for disaster recovery purposes.

d. Records retention is the responsibility of the data owner. Files will need to be kept on the network storage to be included in regular backups or separately archived by the data owner for permanent retention.

3.9 Authorized Software (IT-19)

Users shall accept the responsibility to prevent illegal software usage and abide by university policy on the use of copyrighted materials requiring the university community to respect copyright law.

These responsibilities include:

a. Do not illegally distribute or share software with anyone.

b. All software must be license compliant, including personally purchased software.

c. All software must be installed by IT, unless prior arrangements have been made.

d. All software licenses must be readily available.

e. Report any suspected or known misuse of software to IT by calling (936) 294- 1950, or by emailing servicedesk@shsu.edu.

4. Privacy (IT-27)

You should have no expectation of personal privacy with respect to SHSU information technology resources. Information technology resources provided by SHSU are owned by the State of Texas and subject to state and SHSU oversight. Electronic files and communication created, sent, received, or stored on SHSU information technology resources are not private and may be subject to open records requests.

The use of SHSU information technology resources may be monitored to

manage performance, perform routine maintenance and operations, protect the integrity of SHSU information technology resources, perform security reviews, and fulfill complaint or investigation requirements. For these same purposes, IT may also capture user activity such as websites visited.

5. Physical Security (IT-25)

All information technology resource facilities will be physically protected in proportion to the criticality or importance of their function at SHSU.

1. Access to information technology resource facilities must be granted only to SHSU support personnel and contractors whose job responsibilities require access to that facility and physical access must be documented and managed.
2. Access cards and/or keys must not be shared or loaned to others.
3. Access cards and/or keys that are no longer required must be returned to the person responsible for the facility.
4. Visitors must be escorted in secured areas of information technology resource facilities and visitors access will be logged and tracked (e.g. sign-in / sign-out log book).