SHSU Information Security User Guide

Sam Houston State University

Contents

Section 1: Introduction

1.0 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.

2.0 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@Sam security policies are based on the published Texas Administrative Code, Information Security Standards 1 (TAC § 202), 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@Sam security policies. For ease of inquiry, each section indicates which policy covers that topic.

Policy location: http://shsu.edu/intranet/policies/information_technology_policies/index.html

3.0 Applicability

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

4.0 Users 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 practice standards is mandatory. Your responsibility is to adequately secure information technology resources from unauthorized access, data manipulation, disclosure and theft of sensitive 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.

   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.

3. **It is your responsibility to attend the Security Awareness Training and to familiarize yourself with the SHSU policies** available online at:
   http://shsu.edu/intranet/policies/information_technology_policies/index.html

4. **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.

5.0 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.

6.0 Obtaining a Policy Exemption

Exemptions 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 exemption request.

Section 2: User Security Practices and Safeguards

1.0 User Accounts (IT-01)

1. You will automatically be given an account 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 password and USERID with anyone (including family, friends, co-workers and supervisors).

2.0 Account Passwords (IT-02)

You are responsible for what is accessed, downloaded, or created under your credentials 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.

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

1. Must have a minimum length of six (6) alphanumeric characters.
2. Must contain a mix of upper case, lower case and numeric characters or special characters (!@#%^&*+=?/~';:,<>|\).
3. Passwords must not be easy to guess, for instance, your social security number, your birth date, your nickname, obscenities, etc.
4. Users will be reminded to change passwords at least once per 180 days.
5. Passwords must not be posted on monitors, under keyboards, on sticky notes, etc.
6. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.

3.0 Acceptable Use

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@Sam 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.

3.0.1 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 material that may be offensive, indecent or obscene.

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 must adhere to all the same policies that apply to use from within SHSU facilities.

j. Do not allow family members or other non-employees to access SHSU computer systems.

k. Users must not attach a network device (e.g., a wireless access point) to the university network. (IT-12)

3.0.2 Information Integrity (IT-03)

Users may 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.

3.0.3 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.

3.0.4 Electronic Communication (IT-20)

a. Do not send, forward, or request to receive confidential or sensitive SHSU information through or to non-SHSU E-mail accounts. (such as your account at Hotmail®, Yahoo!® mail, America Online (**AOL**)® mail, etc.)

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

3.0.5 Portable Computing (IT-26)

The users of portable computing devices or media used to store, transmit or process protected 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. Confidential information should not be stored on a portable computing device.

f. 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.

g. Promptly notify IT@Sam if any portable computing device or media has been lost or stolen.

3.0.6 Technology Security Training (IT-13)

a. All employees must complete the SANS security awareness training class within 30 days of being granted access to any SHSU information technology resources and pass the associated examination.

b. All employees must complete the SANs security awareness training annually and pass the associated examination to ensure knowledge is re-enforced on technology security issues.

3.0.7 Computer Virus (Malicious Code) (IT-24)

a. All workstations and laptops must use university approved virus protection software and configuration.

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

c. Viruses that are not automatically cleared by the virus protection software are security incidents and must be reported to Client Services at (936) 294- 1950 or helpdesk@shsu.edu.

3.0.8 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 drive). Local storage is not backed up by IT@Sam.

c. SHSU IT@Sam System Administrators will provide backups and one year retention of data that has been determined critical.

d. Records retention is the responsibility of your department's data owner. If files need to be retained beyond the one year archive, those files will need to be kept on the network storage area to be included in regular backups or separately archived by the data owner for permanent retention.

3.0.9 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@Sam, 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@Sam Client Support Services.

4.0 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@Sam may also capture user activity such as websites visited.

5.0 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 IR facility.
4. Visitors must be escorted in card access controlled areas of information technology resource facilities and visitors will be tracked with a sign in/out log.

This page was intentionally left blank

Section 3: FAQ

1. **What are my responsibilities as a user of SHSU information technology resources?**

   a. Be accountable for your actions regarding technology
   b. Protect SHSU information technology resources by following policies and exercising good judgment.
   c. Know the regulations and policies of SHSU
   d. Take the initial and annual security awareness training
   e. Sign the non-disclosure agreement

2. **Why does my computer have a screensaver time out?**

   The law dictates we all must protect SHSU data. If you do not lock your computer when not in use, a universal security feature will lock it for you after a predetermined amount of time assuming you have left it unattended and unprotected.

3. **Why does my password have to be so complicated?**

   The more complex your password, the less likely someone will guess, or hack, your password and cause damage to SHSU resources in your name, leaving you responsible for the damage.

4. **Why can't I create SHSU documents on Google Docs?**

   Storing SHSU documents that could have the potential for being sensitive or confidential on a public server is an example of using bad judgment in protecting SHSU data. Public servers can be compromised, and IT@Sam has no control over the protection of that data.

5. **Is it OK to forward my SHSU email to my home email account?**

   No, any SHSU email has the potential for containing confidential information. Once the email leaves the security of the SHSU network, it will pass through several public servers as it is routed to your home email, leaving a copy of that email on each unsecure routing server. When that public server is compromised, the SHSU confidential information will also be compromised.

6. **Can I take SHSU documents home on my flash drive to work on at home?**

   It is discouraged. If you have no choice, you must encrypt the drive to protect the data. When in doubt as to the level of confidentiality, err on the side of good judgment and encrypt it. Ask yourself if that information would be ok to be read by anyone if it ended up on the front page of a national newspaper.

7. **I have this great program from home; can I load it on my SHSU PC?**

   All software must be approved and installed by IT@Sam. There are factors to be considered, such as licensing, compatibility, etc. Call the service desk to determine whether it meets the criteria.

8. **Is it ok to access social networking on my university computer?**

   SHSU does not block social networking sites. As long as the time you spend is not excessive (remember to discuss with your supervisor) and it does not interfere with your work. If it becomes a problem, your supervisor can discipline you with substandard job performance.

9. I've lost an SHSU device (phone, laptop, ipad, etc.); what do I do now?

Immediately notify your supervisor and call the service desk. They will initiate the proper process for notifying the Information Security Officer who will notify law enforcement if there is a theft involved.

10. I have accidentally deleted files on my local PC (or laptop); can you restore them?

No. IT@Sam does not back up local workstation or laptop drives. Remember backups are performed in case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors. Restoring a single file or email is a major undertaking, so take care when deleting files.

11. I was perusing the T:\ drive and came upon employee evaluations. Can I read them since they're available to me?

These are categorized as confidential files and should not be accessible to you. Call the helpdesk if this happens, as they will need to initiate the process of informing the systems administrators to correct the error.

12. Can I print out my personal recipes on an SHSU color printer?

Remember that your personal use must not result in direct costs to SHSU. Cost of paper, toner, and wear and tear on the printer is a cost to SHSU.

13. What's wrong with keeping my vacation pictures or music files on my S: drive?

a. You do not want others viewing your pictures for many reasons, to include if someone considers them inappropriate.
b. You are allocated a specific amount of server storage space. If you run out of storage, systems administrators may have to delete pictures or music files to clean it up.
c. The storage space on the server and the backup tapes that your pictures use, result in direct costs to SHSU.

14. I don't like the thought of someone from IT reading my personal documents that are on my S: drive; what can I do?

Do not store personal documents on the server.

15. My co-worker used my PC while it was logged in as me and I was away from my desk; they sent a scathing email to the University President, why am I in trouble?

It is your responsibility to protect the information that you have access to, and locking your machine when you leave your workstation is a vital part of that protection.

16. How was I supposed to know I was supposed to call the service desk if I saw that my anti-virus didn't get rid of that virus?

It is your responsibility to know and understand the policies that govern the use of SHSU information technology resources. This is why familiarizing yourself with SHSU policies and attending the security awareness training is so imperative.

Section 4: Glossary

Glossary

This glossary contains an alphabetized listing of both common and specific terms that are used in the **INFORMATION SECURITY USER GUIDE**.

CONFIDENTIAL INFORMATION
Information maintained by the SHSU that is exempt from disclosure under the provisions of the Texas Public Information Act (*also known as* the Texas Open Records Act) or other state or federal law is confidential.

ELECTRONIC COMMUNICATION
Electronic communication is the transfer of text, html, images, or data through a computer, cell phone, tablet, PDA or any other communication device. This includes E-mail, instant messaging, texting, web pages, blogs and forums.

ENCRYPTION (ENCRYPT, ENCIPHER, OR ENCODE)
The conversion of plaintext information into a secret code that conceals the data's original meaning, and cannot be understood by anyone but the intended recipient.

FLASH DRIVE
A small data storage device that uses flash memory and has a built-in universal serial bus (**USB**) connection; flash drives are typically no more than two or three inches in length and less than an inch in width.

FLASH MEMORY CARD
A solid-state electronic flash memory data storage device. These are mainly used with digital cameras, handheld and mobile computers, mobile phones, music players, digital cinematography cameras, video game consoles, and other electronics.

INCIDENTAL USE
The personal use of the internet on state networks that occurs in incidental amounts of employee time, such as during reasonable convenience breaks.

INFORMATION TECHNOLOGY RESOURCES
Any and all computer printouts, online display devices, magnetic storage media and all computer-related activities involving a device capable of receiving e-mail, browsing websites or otherwise capable of receiving, storing, managing or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (**PDA**s), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (e.g., embedded technology), telecommunications resources, network environments, telephones, fax machines, printers and service bureaus.

INFORMATION RESOURCE MANAGER (IRM)
The individual responsible to the State of Texas for management of the university's information technology resources. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect SHSU information technology resources.

INFORMATION SECURITY OFFICER (ISO)
The employee responsible for administering the information security functions within the university. The ISO is the university's internal and external point of contact for all information security matters.

INTERNET
A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

INTRANET
A network (inernal internet) belonging to an organization accessible only by the organizations employees or others with authorization. An intranet's website looks and acts just like any other web sites, but is protected from unauthorized access by a firewall.

LOCAL AREA NETWORK (LAN)
A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link.

PASSWORD
A string of characters that serves as authentication of a person's identity and may be used to grant, or deny, access to private or shared data.

PORTABLE COMPUTING DEVICE
Any portable device that is capable of receiving and/or transmitting data to and from information technology resources. These include, but are not limited to, notebook computers, handheld computers, PDAs, (personal digital assistants), pagers, cell phones, Universal Serial Bus (**USB**) drives, memory cards, external hard drives, data disks, CDs, DVDs and similar storage.

VIRUS
A program that can replicate itself, spread from one computer to another, and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed.