College of Osteopathic Medicine

Element 9.4: Secure Student Recordkeeping

Sam Houston State University

ELEMENT 9.4: SECURE STUDENT RECORDKEEPING

Sam Houston State University (SHSU) protects the security, confidentiality, and integrity of student records and maintains security measures to protect and back up data. SHSU complies with the *Texas Administrative Code*, Chapter 202, Subchapter B, Rule 202.20 and the Family Education Rights and Privacy Act (FERPA) to ensure the security, confidentiality, and integrity of student records. The University's Academic Policy 810806, Student Educational Records, is established to assure FERPA compliance and designates types, locations, and custodians of various student records. Academic Policy 830823, Reproducing of Hard Copy of Student Academic Records, provides guidelines for the printing of hard copy student academic records.

The University has established an Information Security Program that provides direction for managing and protecting the confidentiality, integrity, and availability of SHSU information technology resources. The program contains administrative, technical, and physical safeguards to protect student and University privileged information. The program defines the roles and responsibilities related to information security, including that of a full-time Information Security Officer (ISO) to oversee the program's various components.

The *SHSU Information Security User Guide* is used as 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. The guide summarizes acceptable practices to educate individuals on the basic responsibilities needed to begin utilizing information resources in a manner that minimizes risks to students and the campus community. Upon employment, computer accounts are created for faculty and staff activation. Activation of these accounts requires the user to agree to abide by the information resources Acceptable Use Policy (IT-03) and users must sign a non-disclosure agreement. Further, in accordance with the Technology Security Training Policy (IT-13) all employees must participate in information security awareness training within 30 days of account activation and then annually thereafter.

Passwords for accounts are regulated by a User Accounts Password Policy (IT-02) that mandates checks to ensure the strength of passwords. Campus users must also change their password on a scheduled basis. Information Technology (IT@Sam) staff members participate in the development of the new employee orientation program conducted by the Department of Human Resources and provide guidance on the use of the University's computer systems. Additionally, new employees receive a document concerning FERPA, which outlines their responsibilities regarding the use of information to which they may have access based on their employment. Access to administrative information systems is controlled by individual username/password authentication. Levels of access within administrative information systems are determined by job duty and individual need and are maintained by the parties responsible for the given data. System access is removed as employees separate from the University.

Access to the online course management system used at SHSU is granted via the same username/password combination as for other administrative information systems. The Information Technology Data Backup and Recovery Policy (IT-11) outlines steps for the protection of information technology data assets. Electronic data is stored on physically and electronically secured servers. Daily backup procedures are in place. Backup tapes are stored in a vault in a building separate from the servers. Academic records that predate electronic storage are retained in a vault within the Registrar's Office. Any student data passed from Banner SIS, the institution's student information system, to Blackboard, the institution's learning management system, is protected. Blackboard is behind a firewall; utilizes the single-sign-on framework provided by IT@Sam for access by students, faculty, and staff; uses role-based permissions to restrict access to data; and is a cloud-hosted solution for backups and redundancy. The Information Technology Data Classification Policy (IT-06) provides a framework for applying the appropriate levels of protection to institutional data based upon proprietary, ethical, operational, and privacy considerations. The policy identifies confidential data that all campus users must protect including, but not limited to, student grades, test scores, usernames, and ID numbers.

Students are informed each semester of their right to privacy via the Schedule of Classes. This information defines the data that are considered to be directory information and as such available for release to the general public. Students may restrict the release of information through requests submitted prior to the census date of the term. These requests may be made either by written notification to the Registrar's Office or through an online program provided for this purpose.

In addition to the student privacy guidelines established by formal policy, the Registrar at SHSU, who serves as the FERPA campus official, publishes additional information and procedures relating to FERPA on the institution's website. Privacy rights webpages are published for the various audiences that may be impacted by or involved with the protection of student privacy and are intended to emphasize key FERPA-related information in an easily digestible manner. Privacy rights webpages exist for the following topics: Family Education Rights and Privacy Act (F.E.R.P.A.), Responsibilities as a Faculty and Staff Member, Responsibilities as a Student Employee, and Parental Access to Children's Education Records.

Regarding the privacy rights webpage that details FERPA, the institution clearly articulates its requirement to "maintain the confidentiality of student educational records." The webpage also reiterates the list of student data that has been established as directory information under FERPA and is included in Academic Policy Statement 810806 and the *Student Handbook*.

In addition to basic FERPA information, the site provides guidance to University personnel in the use of data contained in Banner SIS. Explanations are provided to employees to assist them in recognizing when a student's directory information has been restricted for release. Further, the webpage details actions that are specifically prohibited and defined as violations of FERPA:

- Removing any document from the office for non-business purposes is in violation of FERPA.
- Releasing confidential student information (non-directory) to another student, University organization, or any person who does not have a legitimate educational interest, or parents of a dependent student, without the student's written authorization is in violation of FERPA.
- Leaving reports or computer screens containing confidential student information in view of others who do not have a legitimate educational interest in the data or leaving your monitor unattended is in violation of FERPA.
- Making personal use of student information is in violation of FERPA.
- Allowing another person to use your computer access code is in violation of FERPA.

- Putting paperwork that contains a student's information (e.g., social security number or grades) in the trash is also in violation of FERPA.

Additional student privacy guidelines for institutional personnel are detailed within the *Responsibilities as a Faculty and Staff Member* privacy rights webpage. The webpage reminds faculty and staff that the confidentiality, use, and release of student records are governed by FERPA. In addition, the guidelines inform the faculty and staff of the following:

> . . . All student information must be treated as confidential. Even public or "directory" information is subject to restriction on an individual basis. Unless your job involves the release of information and you have been trained in that function, any requests for disclosure of information, especially from outside the University, should be referred to the Registrar's Office.

The *Responsibilities as a Faculty and Staff Member* privacy rights webpage also reminds faculty and staff of their responsibility for the proper use of their employee computer accounts, passwords, and personal identification numbers in relation to data security. Data security protocols will be addressed in greater depth in the following sections of this narrative.

Much like the privacy rights webpage for faculty and staff, the *Responsibilities as a Student Employee* webpage exists for student employees. The webpage details the following student privacy expectations:

- No one may make or permit unauthorized use of any information in files maintained, stored, or processed by the office in which they are employed.
- No one is permitted to seek personal benefit or to allow others to benefit personally by knowledge of any confidential information which has come to them by virtue of their work assignment.
- No one is to exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and in accordance with University policies and procedures.
- No one may knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry. No one may knowingly expunge, or cause to be expunged, in any record or report, a data entry.
- No official record or report, or copy thereof, may be removed from the office where it is maintained except in the performance of a person's duties.
- No one is to aid, abet, or act in conspiracy with another to violate any part of this code.
- Any knowledge of a violation must be immediately reported to the person's supervisor.

In addition to faculty, staff, and student employee expectations, a privacy rights webpage addresses parental access to student educational records. The *Parental Access to Children's Education Records* webpage informs parents and employees that parents have no inherent right to inspect a student's education records.

Finally, both the Student Health Center and the Student Counseling Center take steps to protect the security, confidentiality, and integrity of student records, which are retained per SHSU and state regulations. The Student Health Center follows specific policies related to access to patient information, as well as the retention and disposal of patient records. Adult records are kept for 7 years from the date of the last treatment, and minor patient records are retained for 7 years after the date of the last treatment or until the patient reaches age 21, whichever date is later. The Student Counseling Center also takes steps to maintain student confidentiality. Staff members are not allowed to discuss confidential client information with anyone outside of the Counseling Center unless a signed release of information form has been signed by the client. The form must be signed and dated by the client, as well as by a witness other than the counselor named in the release.

<<Prev Rule Next Rule>>

Texas Administrative Code

TITLE 1	ADMINISTRATION
PART 10	DEPARTMENT OF INFORMATION RESOURCES
CHAPTER 202	INFORMATION SECURITY STANDARDS
SUBCHAPTER B	INFORMATION SECURITY STANDARDS FOR STATE AGENCIES
RULE §202.20	Responsibilities of the Agency Head

The head of each state agency is ultimately responsible for the agency's information resources. The head of each state agency or his/her designated representative(s) shall:

(1) designate an Information Security Officer who has the explicit authority and the duty to administer the information security requirements of this chapter agency wide;

(2) allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the agency head;

(3) ensure that senior agency officials and information-owners, in collaboration with the Information Resources Manager and Information Security Officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control;

(4) ensure that the agency has trained personnel to assist the agency in complying with the requirements of this chapter and related policies;

(5) ensure that senior agency officials support the agency Information Security Officer in developing, at least annually, a report on agency information security program, as specified in §202.21(b)(11) and §202.23(a) of this chapter;

(6) approve high level risk management decisions as required by §202.25(4) of this chapter;

(7) review and approve at least annually the agency information security program required under §202.24 of this chapter; and

(8) ensure that information security management processes are integrated with agency strategic and operational planning processes.

Source Note: The provisions of this §202.20 adopted to be effective March 17, 2015, 40 TexReg 1357

List of Titles Back to List

HOME | TEXAS REGISTER | TEXAS ADMINISTRATIVE CODE | OPEN MEETINGS

Skip to main content | About Us | Contact Us | FAQs | Language Assistance

U.S. Department of Education

Search... Search

Student Loans | Grants | Laws | Data

LAWS & GUIDANCE / GENERAL

Family Educational Rights and Privacy Act (FERPA)

Get the Latest on FERPA at https://studentprivacy.ed.gov/

- **Frequently Asked Questions**
- FERPA for **parents and students**, **K12 school officials** and **Postsecondary school officials**
- Protection of Pupil Rights Amendment (**PPRA**)
- **Guidance and Notices**

Family Policy Compliance Office (FPCO) Home

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and

How Do I Find...

- Student loans, forgiveness
- College accreditation
- Every Student Succeeds Act (ESSA)
- FERPA
- FAFSA

More >

Information About...

- Transforming Teaching
- Family and Community Engagement
- Early Learning

Related Topics

- **Key Policy Letters**

- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information, you may call 1-800-USA-LEARN (1-800-872-5327) (voice). Individuals who use TDD may use the Federal Relay Service.

Or you may contact us at the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-8520

□ Printable view

Last Modified: 03/01/2018

Student Loans
Repaying Loans
Defaulted Loans
Loan Forgiveness
Loan Servicers

Grants & Programs
Apply for Pell Grants
Grants Forecast
Apply for a Grant
Eligibility for Grants

Laws & Guidance
Every Student Succeeds Act (ESSA)
FERPA
Civil Rights
New IDEA Website

Data & Research
Education Statistics
Postsecondary Education Data
ED Data Express
Nation's Report Card
What Works Clearinghouse

About Us
Contact Us
ED Offices
Jobs
Press Releases
FAQs
Recursos en español
Budget, Performance
Privacy Program
Subscribe to E-Mail Updates

Notices FOIA Privacy Policy Accessibility Security Information quality Inspector General Whitehouse.gov USA.gov
Benefits.gov Regulations.gov

1. PURPOSE

This policy is established to assure compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA).

2. DEFINITIONS

For purposes of this policy, Sam Houston State University provides the following definitions:

2.01 Student - An individual who is receiving or has received instruction in a course, including an activity which is evaluated towards a grade such as classroom instruction, an academic internship, a student teaching assignment, or a correspondence course.

2.02 Educational Record - Any record maintained by Sam Houston State University, an employee of the University, or an agent of the University which is directly related to a student or former student, EXCEPT:

a. A personal record kept by a University staff person or agent, which meets the following tests:

(1) It was made as a personal memory aid and

(2) It is in the sole possession of the person who made it.

b. An employment record used only in relation to an individual's employment by Sam Houston State University. However, the records of a student's employment are educational records when:

(1) The position in which the student is employed depends on his/her status as a student, or

(2) The student receives a grade or credit based on his/her performance as an employee.

c. Records connected with individuals applying for admission to Sam Houston State University, who do not enroll at the University.

d. Records maintained by Sam Houston State used only for the provision of medical, psychiatric, psychological or other recognized professional treatments that are otherwise protected by a privilege recognized by State law. In order to maintain these records separate from educational records, Sam Houston State University will enforce the following conditions:

(1) No person other than the physicians, psychiatrists, psychologists, or other recognized professionals providing treatment will have access to information contained in the Health Center records. Such records, however, may be disclosed to other persons under the procedures to meet a health and safety emergency as described in the FERPA and this policy.

(2) Personal Identifier - Any data or information that relates a record to an individual. This includes the individual's name, the name of the individual's parents or other family members, the individual's addresses (permanent or present), the individual's social security number, any other number or symbol which identifies the individual, a list of the individual's personal characteristics, or any other information which would make the individual's identity known and can be used to label a record as the individual’s.

3. ANNUAL NOTIFICATION

Sam Houston State University publishes in the student *Guidelines* bulletin provided each student at orientation and registration a notice to students of their rights under the FERPA. The notice will include, but not be limited to, the following:

3.01 The right of a student to inspect and review his/her educational record.

3.02 The intent of Sam Houston State University to limit the disclosure of information contained in a student's educational records to the following circumstances:

a. With the student's prior written consent,

b. As an item of directory information which the student has not refused to permit the University to disclose, or

c. Under the FERPA provisions which allow a university to disclose information without the student's prior consent.

3.03 The right of a student to petition Sam Houston State University to amend or correct any part of his/her educational record which he/she believes is inaccurate, misleading, or in violation of the privacy or other rights of students. When the University decides it will not amend or correct a student's record, the student has a right to a hearing to present evidence that the record is inaccurate, misleading, or in violation of the privacy or other rights of students.

3.04 The right of any person to file a complaint with the Family Policy Compliance Office of the U.S. Department of Education if Sam Houston State University violates the FERPA.

3.05 The procedure which a student should follow to obtain a copy of this policy and the locations where a student may obtain a copy.

4. STATEMENT OF RIGHTS

4.01 Sam Houston State University encourages students to exercise all of their rights under the Family Educational Rights and Privacy Act and this policy.

Since a student's educational record will be used repeatedly by University officials and others to make important decisions affecting the student's academic program and future career, the student should assume a personal responsibility to make certain that his/her record is complete and accurate.

4.02 This policy is intended to inform each student about Sam Houston State University's procedures to provide students with their rights to:

a. Inspect and review their educational records.

b. Exercise control (with some limitations) over disclosure of information contained in their educational records.

c. Seek to correct their educational records, in a hearing if necessary, when they believe their records are inaccurate, misleading, or in violation of the privacy or other rights of students.

d. Report violations of the FERPA to the Family Policy Compliance Office of the U.S. Department of Education.

e. Be informed about their FERPA rights.

4.03 Sam Houston State University has placed responsibility for administration of the FERPA with the appropriate custodian of educational records. Each custodian is responsible for the administration of this policy. Students who have problems or questions related to the policy should contact the appropriate educational record custodian for help.

5. LOCATIONS OF EDUCATIONAL RECORDS

Types	Office	Custodian
Admissions Records	Admissions Office	Director, Undergraduate Admissions
Cumulative Academic Records	Registrar’s Office	Registrar
Health Records	Health Center	Administrator, University Health Center
Financial Aid Records	Financial Aid Office	Director, Financial Aid
Public Safety Service Records	Public Safety Services	Director, Public Safety Services
Financial Records	Cashier’s Office	Office Manager, Cashier’s Office
Placement Records	Career Services	Director, Career Services
Counseling Records	Counseling Center	Director, Counseling Center
Disciplinary Records	Student Life Office	Dean of Students
Occasional Records (Student educational records included in the types of systems listed above such as minutes of faculty committee meetings, copies of correspondence in offices listed, etc.)	The FERPA Coordinator will collect such records, direct the student to their location, or otherwise make them available for inspection and review	The University staff person who maintains such occasional records
Advising Records	Student Advising and Mentoring Center	Executive Director/SAM Center

6. PROCEDURE TO INSPECT EDUCATIONAL RECORDS

6.01 Sam Houston State University permits students to inspect and review their educational records. Students who wish to inspect and review their records should submit a written request to the record custodian. The request should identify as accurately as possible the specific records the student wishes to inspect and review. The request may identify records according to the types listed in this policy under "Location of Educational Records" or as records under the custodianship of specific University officials identified by title.

6.02 If it is mutually convenient, the record custodian will allow the student to inspect the records at once. If the student cannot inspect the records immediately, the official responsible for responding to the request will arrange a time convenient to both the student and the custodian for inspecting the records. In no case will the time designated for inspection be more than 45 days after the request for inspection has been made.

6.03 When a record contains personally-identifiable information about more than one student, a student may inspect only that information which relates to him/her.

6.04 Sam Houston State University reserves the right to refuse to permit a student to inspect and review the following educational records:

a. The financial statement of the student's parents or legal guardian.

b. Statements and letters of recommendation prepared by University officials or others which were placed in the student's records before January 1, 1975, or for which the student has waived his/her right of access, provided the letters and statements are used only for the purposes for which they were specifically intended.

c. Those records which are excluded from the FERPA definition of educational records (see "Definitions" in Section 2).

7. FEES FOR COPIES OF RECORDS

7.01 Sam Houston State University will charge the following fees for copies of the educational records:

a. Official Transcripts - Students will be charged per University policy as outlined on the Registrar's homepage.

b. FERPA requires copies of educational records - The law requires the University to provide copies of educational records to students when

(1) A failure to do so would effectively deny the student the right to inspect and review his/her record.

(2) The University has disclosed information from the student's educational record under authority of the student's prior written consent and the student requests a copy of the information disclosed.

(3) The student requests copies of records the University has disclosed to other schools where the student seeks or intends to enroll.

7.02 Sam Houston State University reserves the right to deny transcripts or copies of records not required by the FERPA in any of the following situations:

a. The student has an unpaid financial obligation to the University.

b. There is an unresolved disciplinary action against the student.

c. While there is unresolved litigation between the student and the University.

8. DIRECTORY INFORMATION

8.01 Sam Houston State University proposes to designate the personally-identifiable information contained in a student's educational record listed below as "directory information" in order that the University may, at its discretion, disclose the information without a student's further prior written consent:

a. The student's name
b. The student's local and home address
c. The student's major
d. The student's minor
e. The student's local and home telephone numbers

f. The student's degrees, diplomas, and certificates and dates of award
g. The student's honors and awards
h. The student's classification
i. The student's extracurricular activities
j. The student’s birth date and place of birth
k. Names and addresses of parents or legal guardians of the student
l. Weight, height, and related information of athletic team members
m. The student's age, race, sex, and marital status
n. The student’s e-mail address

8.02 Within the first month of each academic semester, the Registrar will publish in *The Houstonian* the above list of items of directory information it proposes to designate as directory information.

8.03 After the students have been notified by the announcement in the newspaper, they will have the first twelve class days in a long semester or the first four class days in a summer session to change their directory information release status via the web.

8.04 The Registrar will notify the appropriate custodians of educational records of a student's refusal to permit the University to designate an item of information as directory information to be released. The custodians will mark their records accordingly. They will not make any further disclosures of those items of information about the student without the student's prior written consent except to parties who have legal access to student records without written consent.

8.05 The appropriate custodians of records are authorized to disclose directory information.

9. USE OF STUDENT EDUCATIONAL RECORDS

9.01 All officials of Sam Houston State University will follow a strict policy that information contained in a student's educational record is confidential and may not be disclosed to third parties without the student's prior consent (written or electronic) except as otherwise provided in this section of Sam Houston State University's Student Educational Records Policy.

9.02 The University maintains student educational records in order for the administrative staff and the faculty to perform their proper functions to serve the student body. To carry out their responsibilities, these officials will have access to student educational records for legitimate educational purposes.

9.03 To establish who are University officials having access to educational records, Sam Houston State University will apply the criteria listed below. A "University official" includes:

a. A member of The Texas State University System Board of Regents.

b. Any and all persons employed by The Texas State University System or Sam Houston State University.

c. A person under contract to The Texas State University System or Sam Houston State University to perform a specific task where, by law or contract, the System or the University has the right to control access to the educational records.

9.04 University officials who meet the criteria listed above will have access to personally-identifiable information contained in student educational records if they have a legitimate educational interest in doing so. A "legitimate educational interest" is the person's need to know in order to:

a. Perform an administrative task which is outlined in the official position description or contract of the individual or which is otherwise related to the individual's position and duties.

b. Perform a supervisory or instructional task directly related to the student's education.

c. Perform a service or benefit for the student such as health care, counseling, student job placement, or student financial aid.

9.05 Within the general policy that University officials must secure a student's prior written consent before they disclose personally-identifiable information contained in the student's educational records, Sam Houston State University reserves the right for its officials to make such disclosures without the student's consent in the following circumstances:

a. When the student seeks or intends to enroll in another college or university.

b. When certain federal and state officials request information in order to audit or enforce legal conditions related to federally-supported educational programs in the University.

c. To parties who provide or may provide financial aid to the student in order to:

(1) Establish the student's eligibility for the financial aid.
(2) Determine the amount of financial aid.
(3) Establish the conditions for the receipt of the financial aid.
(4) Enforce the terms of the agreement between the provider and the receiver of the financial aid.

d. To state and local officials or authorities to whom information is specifically required to be reported or disclosed pursuant to any state status adopted prior to November 19, 1974.

e. To organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction; provided that the studies are conducted in a manner which will not permit the personal identification of students and their parents by individuals other than representatives of the organization and the information will be destroyed when no longer needed for the purposes for which the study was conducted.

f. To accrediting organizations to carry out their accrediting functions.

g. To parents/legal guardians of a student if the parents claim the student as a dependent under the Internal Revenue Code of 1954. Sam Houston State University will exercise this option only on the condition that evidence of such dependency is furnished to the custodian of records. It is generally held that FERPA rights of eligible students lapse or expire upon the death of the student.

h. To comply with a judicial order or lawfully issued subpoena. The University will make a reasonable effort to notify the student before it makes a disclosure under this provision.

9.06 Sam Houston State University authorizes its officials to make the needed disclosures from student educational records in a health or safety emergency if the official deems:

a. The disclosure to be warranted by the seriousness of the threat to the health or safety of the student or other persons.

b. The information to be necessary and needed to meet the emergency.

c. Time to be an important and limiting factor in dealing with the emergency.

9.07 Officials of Sam Houston State University may not disclose personally-identifiable information contained in a student's educational record except directory information or under the circumstances listed above except with the student's prior written consent. The written consent must include at least:

a. A specification of the information the student consents to be disclosed,

b. The purpose for which the disclosure may be made,

c. The person or organization or the class of persons or organizations to whom the disclosure may be made, and

d. The date of the consent and, if appropriate, a date when the consent is to be terminated.

9.08 The student may obtain a copy of any record the University discloses by the student's prior written consent.

9.09 Sam Houston State University will not release information contained in a student's educational records, except directory information, to any third parties except its own officials, unless those parties agree that they will not redisclose the information without the student's prior written consent.

10. RECORDS OF REQUEST FOR ACCESS AND DISCLOSURES MADE FROM EDUCATIONAL RECORDS

Sam Houston State University will maintain a record of each request granted or rejected and each disclosure of personally-identifiable information from the educational records of the student that indicates:

a. The name of the person or agency that made the request.

b. The interest the person or agency had in the information.

c. The date the person or agency made the request.

d. Whether the request was granted and, if it was, the date access was permitted or the disclosure was made. The University will maintain this record of disclosure as long as it maintains the student's educational record.

11. PROCEDURES TO SEEK CORRECT EDUCATIONAL RECORDS

11.01 Request for Correction - The University will permit students to challenge the content of their educational records to ensure that records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of students. (Note: Under the FERPA, the University is permitted to refuse to consider a student's request to change the grade an instructor assigns for a course.)

11.02 For purposes of outlining the procedure to seek to correct educational records, the term "incorrect" will be used to describe a record that is inaccurate, misleading, or in violation of the privacy or other rights of a student. Also, in this section, the term "requester" will be used to describe a student or former student who is asking the University to correct a record.

11.03 If a student or former student discovers an incorrect item in his/her educational record, he/she should informally discuss the problem with the record custodian. If the custodian finds the record is incorrect because of an obvious error, and it is a simple matter to correct it to the satisfaction of the requester, the custodian may make the change.

11.04 If the custodian cannot change the record to the requester's satisfaction or the record does not appear to be obviously incorrect, the custodian will:

a. Provide the requester a copy of the questioned record at no cost and

b. Ask the requester to initiate and provide the custodian a written request for the change.

11.05 The written request should at least identify the item the requester believes is incorrect and state whether it:

a. Is inaccurate and why,

b. Is misleading and why, or

c. Violates the privacy or other rights of students and why. The requester must date and sign the request.

11.06 The record custodian will then amend the educational record of the student or refuse to amend it. The record custodian shall notify the requester of the refusal and advise the requester of the right to a hearing.

11.07 The hearing - The hearing will be held within a reasonable period of time and it will be conducted by an impartial University official appointed by the President. The requester may have anyone of his/her choice, including an attorney, at the hearing. If the requester is not satisfied with the result of the hearing, he/she may file a grievance with the Family Policy Compliance Office of the U.S. Department of Education. If the requester does not agree with the University's interpretation of the requester's record, the requester may file his/her own interpretation. The requester's interpretation will be placed with his/her educational record and maintained by the University. The University will provide the interpretation of the student and the interpretation of the University with the educational record of the student.

12. ADOPTION

12.01 The Student Educational Records Policy was adopted by Sam Houston State University and became effective August 17, 1981.

12.02 Copies of this policy will be available for student review online and in the Newton Gresham Library.

12.03 Free copies will be available to students upon request at the Registrar's Office.

APPROVED: /signed/
James F. Gaertner, President

DATED: 10/21/08

CERTIFICATION STATEMENT

This academic policy statement (APS) has been approved by the reviewer(s) listed below and represents Sam Houston State University's Division of Academic Affairs' APS from the date of this document until superseded.

Original Date: August 6, 1981 Review Cycle: August, ONY*
Reviewer(s): Academic Policy Council Review Date: August 1, 2009

Approved: /signed/ Date: 10/20/08
David E. Payne
Provost and Vice President
for Academic Affairs

*ONY = Odd Numbered Year

Sam Houston State University
Academic Policy Statement 830823
Reproducing of Hard Copy of Student Academic Records
from the University’s Computer Data Bank
Page 1 of 3
Revised May 4, 2005

1. PURPOSE

The purpose of this policy is to establish guidelines for the printing of hard copy student academic records from the university's computer data bank.

2. COMPLIANCE WITH FAMILY EDUCATION RIGHTS AND PRIVACY ACT OF 1974 (FERPA)

2.01 University or System officials having a "legitimate educational interest" in student educational records may have access to those records in order to carry out their official responsibilities at Sam Houston State University.

2.02 A "legitimate educational interest" is defined as a person's need to access student educational records in order to perform:

a. An administrative task which is outlined in the official position description or contract of the individual or which is otherwise related to the individual's position or duties;

b. A supervisory, advisory, or instructional task directly related to the student's education; or

c. A service or benefit for the student such as health care, counseling, student job placement, or student financial aid.

d. Any other task, function, or duty permitted by the Family Educational Rights and Privacy Act.

3. CUSTODIAN OF STUDENT EDUCATIONAL RECORDS

3.01 The President of Sam Houston State University or his/her designee is the custodian of all University records.

3.02 The Registrar serves as custodian of student academic records as the President’s designee and is responsible to the President for:

a. Maintaining accurate student academic records.

b. Security of said records.

c. Ensuring that student's official academic records on file in the Registrar's Office are issued only to those having a "legitimate educational interest" in said records.

4. GUIDELINES TO BE FOLLOWED WHEN HARD COPY STUDENT ACADEMIC RECORDS ARE PRINTED FROM THE UNIVERSITY'S COMPUTER DATA BANK

4.01 Access codes will be restricted to authorized university officials.

4.02 University or System officials will not provide hard copies of student academic records to students.

4.03 Students may obtain official transcripts from the Registrar's Office for an appropriate fee provided there is no hold on their receipt of such transcript (e.g., delinquent student loan); further, that students are entitled under the State Public Information Act to an unofficial transcript.

4.04 The following third party message appears on the hard copy of any student's academic record retained in the office of university officials in order to relieve the President and the Registrar from liability should the record fall into unauthorized hands and legal action result.

Confidential. Release of information contained on this document without the written consent of the person(s) identified on the document is in violation of Sec. 438 Public Law 90-247," the Family Educational Rights and Privacy Act and the Texas Public Information Act, Government Code, Chapter 552.

4.05 Said records must be destroyed when no longer needed.

APPROVED: /signed/
James F. Gaertner, President

DATED: 05/06/05

CERTIFICATION STATEMENT

This academic policy statement (APS) has been approved by the reviewer(s) listed below and represents Sam Houston State University's Division of Academic Affairs' APS from the date of this document until superseded.

Original Date:	August 23, 1983	Review Cycle:	August, ONY*
Reviewer(s):	Academic Policy Council	Review Date:	August 1, 2007

Approved: /signed/ Date: 05/25/05
David E. Payne
Provost and Vice President
for Academic Affairs

*ONY = Odd Numbered Year

Sam Houston State University

Information Security Program

2014

TABLE OF CONTENTS

Overview

Introduction

The Sam Houston State University (SHSU) Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of SHSU information technology resources.

The Information Security Program contains administrative, technical, and physical safeguards to protect university information technology resources. Measures shall be taken to protect these resources against accidental or unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to SHSU information technology resources shall be appropriately managed by the SHSU Information Security Program. Unauthorized modification, deletion, or disclosure of information technology resources can compromise the mission of SHSU, violate individual privacy rights, and possibly constitute a criminal act. (TAC§202.70).

This framework represents the basis of the institutional information security program and on the aggregate whole meets the objectives as articulated by TSUS Rule III, paragraph 19 and its associated guidelines. The SHSU Information Security Program and security standards are not intended to prevent or impede the authorized use of information technology resources as required to meet the university mission.

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

Purpose

The purpose of the SHSU Information Security Program is to provide the university community with a description of the university strategic plan for achieving compliance with information security related laws and guidelines. Additionally the framework of this plan is designed to document the controls used to meet the information security program objectives by:

- Identifying system data owners, providing the data classification standard and identifying the category of its data.
- Reviewing all authorized users and their security access for each system.
- Providing security awareness training for all employees.
- Performing the risk assessment process and developing the risk mitigation plan.
- Reviewing and updating the disaster recovery plan.
- Reviewing current policies and training program.
- Creating a security effectiveness report to the president.
- Reviewing the current process and implement changes as necessary.

The Information Security Program process combines multiple security elements into a management framework that supports the objectives of confidentiality, integrity, and availability.

Authority

1 Texas Administrative Code (TAC) §202
Texas State University System (TSUS) Rules and Regulations

Scope

This program applies equally to all individuals granted access privileges to any Sam Houston State University information technology resource, to include the following:

- Central and departmentally-managed university information technology resources.
- All users employed by SHSU, contractors, vendors, or any other person with access to SHSU's information technology resources.
- Non-SHSU-owned computing devices that may store protected SHSU information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, network resources owned or managed by SHSU. This includes third party service providers' systems that access or store SHSU's protected information.
- Auxiliary organizations, external businesses and organizations that use university information technology resources must operate those assets in conformity with the SHSU Information Security Program.

Information Security Roles and Responsibilities

The following distinctions among owner, custodian, and user responsibilities guide determination of the roles: (TAC§202.71(c)).

Data Owner

The owner or his or her designated representative(s) are responsible for and authorized to:

- Approve access and formally assign custody of information technology resources.
- Determine the asset's value.
- Specify data control requirements and convey them to users and custodians.
- Specify appropriate controls, based on a risk assessment, to protect the state's information technology resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information technology resources and services outsourced by the institution of higher education.
- Confirm that controls are in place to ensure the confidentiality, integrity, and availability of data and other assigned information technology resources.
- Assign custody of information technology resources and provide appropriate authority to implement security controls and procedures.
- Review access lists based on documented security risk management decisions.
- Approve, justify, document, and be accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the ISO or other person(s) designated by the state institution of higher education head.
- The information owner, with the concurrence of the institution of higher education head or his or her designated representative(s), is responsible for classifying business functional information.

SHSU Data Owners:

- Finance and Operations, VP Finance and Operations
- Student and Enrollment Management, VP Enrollment Management
- Academic Affairs, Associate Provost
- Banner General, Designated IRM

Data Custodian

Custodians of information technology resources, including third-party entities providing outsourced information technology resources services to state institutions of higher education shall:

- Implement the controls specified by the information owner(s);
- Provide physical, technical, and procedural safeguards for the information technology resources;
- Assist information owners in evaluating the cost-effectiveness of controls and monitoring; and
- Implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

SHSU Data Custodians:

- Graduate Admissions: Director of Projects
- Undergraduate Admissions: Director
- Purchasing: Director of Procurement and Business Services
- Budgeting: AVP Budget and Operations
- Student Records: Registrar
- Banner General: Director ERP Services
- Financial Aid: Director of Financial Aid
- Residence Life: Director of Residence Life
- Human Resources: Director of Human Resources
- Payroll: Manager
- Accounting, Cashier, Accounts Payable: Controller

Users

Users of information technology resources shall use the resources only for defined purposes and comply with established controls.

Information Security Officer (ISO)

Each institution of higher education head or his or her designated representative(s) shall designate an ISO to administer the University Information Security Program. The ISO shall report to executive management.

- It shall be the duty and responsibility of this individual to develop and recommend policies and establish procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information technology resources assets against unauthorized or accidental modification, destruction, or disclosure.
- The ISO shall document and maintain an up-to-date Information Security Program. The Information Security Program shall be approved by the institution of higher education head or his or her designated representative(s).
- The ISO is responsible for monitoring the effectiveness of defined controls for mission critical information.
- The ISO shall report, at least annually, to the institution of higher education head or his or her designated representative(s) the status and effectiveness of information technology resources security controls.

- The ISO with the approval of the institution of higher education head or his or her designated representative may issue exceptions to information security requirements or controls. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

Information Resources Manager (IRM)

The SHSU Information Resources Manager (IRM) is the duty of the Vice President for Information Technology (VPIT), also known as the Chief Information Officer (CIO), who is responsible to the State of Texas for management of the agency's information resources. The designation of an agency Information Resources Manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. 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 the Information Resources of the agency.

Program Framework

This section defines the Information Security Program process that will ensure the continuity, performance and security of SHSU's information systems. This framework is based on the main objective of the information security program: confidentiality, integrity, and availability.

A review of SHSU's Information Security Program for compliance with required standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the Information Security Program (TAC§202.71(e).

The following processes will ensure that the appropriate safeguards are applied to SHSU's information systems and will continue to mature with the growing needs of the university's mission.

1. Establish Responsibility

At the beginning of each fiscal year, the assigned data owners and their selected data custodians will be reviewed by the IRM and the ISO per IT-05 Data Access Review Policy. The data owners will review/identify the related data stored on their system and identify the categories of data stored as confidential, protected or public according to the data classification standards in IT-06 Data Classification Policy. The data owners will then review the list of authorized users for each system and make the necessary changes using the least privileged model.

The IRM will review and approve information ownership and responsibilities to include personnel, equipment, hardware and software, as well as define information classification categories. (TAC§202.71(a)(b)).

2. Security Awareness Training

All employees with access to the SHSU information technology resources must participate in information security awareness training (IT-13 Technology Security Training Policy) (TAC§202.77). The training promotes awareness of:

- SHSU information security policies, standards, procedures, and guidelines.
- Potential threats against university protected data and information technology resources.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information technology resources.

New employees will sign a non-disclosure agreement and will be provided individual access to the Information Security Awareness Training Program.

Employees are expected to complete the training within 30 days of receiving their access to the program, and then annually.

Department heads and university executive management are responsible for and will be provided status of training compliance.

3. Risk Assessment and Planning

Risk Planning

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Understanding risk, especially the magnitude of the risk, allows organizations to prioritize resources.

Security must be a consideration from the very beginning of any project at the university rather than something that is added later.   A control review should be performed before implementation of information technology resources which store or handle confidential, sensitive, and/or protected information. This may include:

- A technical security evaluation to ensure appropriate safeguards are in place and operational.
- A risk assessment, including a review for regulatory, legal and policy compliance.
- A contingency plan, including the data recovery strategy.
- A review of on-going production procedures, including change controls and integrity checks.

Risk Assessment

SHSU performs annual assessments of its information risks and vulnerabilities (IT-17 Risk Assessment Policy). Risk assessments may be aimed at particular types of information, areas of the organization, or technologies. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of university controls. Risk assessments shall:

- assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- evaluate the sufficiency of existing policies, procedures, information systems, internal controls and security practices, in addition to other safeguards in place to control risks;

- be classified and updated based on the inherent risk. Risk and frequency will be ranked 'high', 'medium', or 'low' based on TAC§202.72 criteria;
- design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of state and federal laws;
- monitor the effectiveness of those safeguards;
- analyze data collected to identify control objectives, risk exposures, mitigation strategies and action plans for addressing each risk with timelines; and
- support the annual report to the president and substantiate any changes to the information security program that may be needed as a result of evaluating the information collected.

4. Disaster Recovery/Business Continuity Plan

IT@Sam is responsible for developing and maintaining a Disaster preparedness/ Recovery/ Business Continuity Plan designed to address the operational restoration of SHSU's critical computer processing capability. This plan identifies the strategy to recover centrally administered data storage, programs, and processing capability in the event of a disaster. The plan identifies the minimum acceptable recovery configuration, which must be available for SHSU to resume the minimum required levels of essential services. The plan is located in strategic areas and available to all Computer Services personnel through a shared network resource. The plan contains proprietary and confidential information, is not intended for public distribution, and will not be published on the Web in its entirety. (TAC§202.74 and Texas Government Code 552.139) (Texas Government Code, Sec. 552.139)

The IT@Sam Disaster Preparedness/Recovery Plan described above does not address the needs of individual departments beyond the restoration of access to their critical centrally administered applications. All major university divisions/departments develop individual plans for protecting their information resource assets and operating capability. Each departmental plan will address losses ranging from minor temporary outages to catastrophic.

5. Annual Review

At the end of each fiscal year, the Information Security Officer (ISO) will review the risk assessment results, Security Awareness Training Program, Information Security User Guide, Information Security Program and all SHSU IT Policies.

The ISO and IRM will report the status and effectiveness of SHSU's information security controls and will present recommended revisions and improvements based on the information collected. The report will include:

- Description and/or narrative of any security incident that resulted in a significant impact to the university.
- Status of the Risk Assessments noting any significant changes.
- Status of the Vulnerability Assessments noting any major findings and corrections.
- Status of the IT Policy review.
- Status of the IT Security Awareness Training Program.
- Anticipated changes in the next fiscal year.

Compliance References

SHSU's information security practices must comply with a variety of federal and state laws, and SHSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver's license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

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 to the use of institutional information technology resources are listed below.

To avoid breaches of any law, regulation, contractual obligation, or institutional policy, information technology resources will be regularly tested and audited to assure adherence with both external and internal standards.

Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of the institution's information technology resources.

- 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
- 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
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

Failure to Comply (Enforcement)

Consistent with SHSU policies, the ISO is authorized by the President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the University community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

SHSU reserves the right to temporarily or permanently suspend, block, or restrict access to university information technology resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of SHSU information technology resources; to protect SHSU from liability; or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement 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 TAC§202.77.

The VPIT or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate university officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to SHSU.

Appeals of university actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for SHSU students and employees.

Obtaining a Policy Exemption

Exemptions to policies are granted on a case-by-case basis and must be reviewed and approved by the university designated IRM. The IRM will mandate the documentation and additional administrative approvals required for consideration of each policy exemption request. TAC§202.71(c)(1)(H) and (d)(5).

Definitions

Contains an alphabetized listing of both common and specific terms that are used in this Information Security Program.

Availability – Ensuring that information systems and the necessary data are available for use when they are needed.

Business Continuity Plan - A plan to ensure that the essential business functions of the organization are able to continue (or re-start) in the event of unforeseen circumstances. The BCP will identify the critical people (roles / functions), information, systems and other infrastructure, e.g. telephones, which are required to enable the business to operate. A detailed plan will be laid out and, if called upon, should be executed to assure minimum additional disruption.

Confidentiality – Assurance that information is shared only among authorized persons or organizations.

Data Custodian – The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

Data Owner – departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Disaster Recovery Plan - The plan that is activated when there is an emergency which ensures that health and safety come first followed by damage limitation. Having contained the impact of the disaster, and having ensured that the situation is under control e.g. through the Emergency Services, then the Business Continuity Plan will be activated.

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

Information Security – The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

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

Information Security Program – Program that contains administrative, technical, and physical safeguards to protect information technology resources.

Integrity – Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Mitigate – The effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Remediate – The act or process of correcting a fault or deficiency.

Risk – The likelihood that something bad will happen that causes harm to, or loss of, an information asset.

Risk Assessment – A systematic process of evaluating the potential risks that may be involved in the use of the SHSU information technology resources.

Security Incident - A security incident is a computer, network, or paper based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

Threat – Anything that has the potential to cause harm.

User – Person responsible for viewing, amending and updating the content of the SHSU information assets.

Vulnerability – A weakness that could be used to endanger or cause harm to an information asset.

Vulnerability Assessment - the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Appendix A – Presidential Approval of Information Security Program

Sam Houston State University
Memorandum

To:	Dr. Dana L. Gibson President	Date:	June 10, 2014
From:	Mark Adams Chief Information Officer	Subject:	Information Security Program Presidential Approval

This memorandum requests formal approval of the updated Information Security Program. (ver 2014-03-31).

Background

Based on the 2009 Texas State University System Rules (TSUS) Audit Findings verifying compliance with the TSUS Rules and Regulations and the Texas Administrative Code (TAC 202) Subchapter C, the Information Security Program developed in 2012 (ver 2012-08-30) was updated. The updated document was reviewed and approved by the Information Security Officer and Information Resource Manager and forwarded to the President for approval.

Approval

I approve the Information Security Program (copy attached) which provides a general framework for Information Security and assures our compliance with the Texas State University System Rules and Regulations and TAC 202 Subchapter C.

Signed Dana ______________________ Date 6/11/14

Dana Gibson, President

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), 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@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.

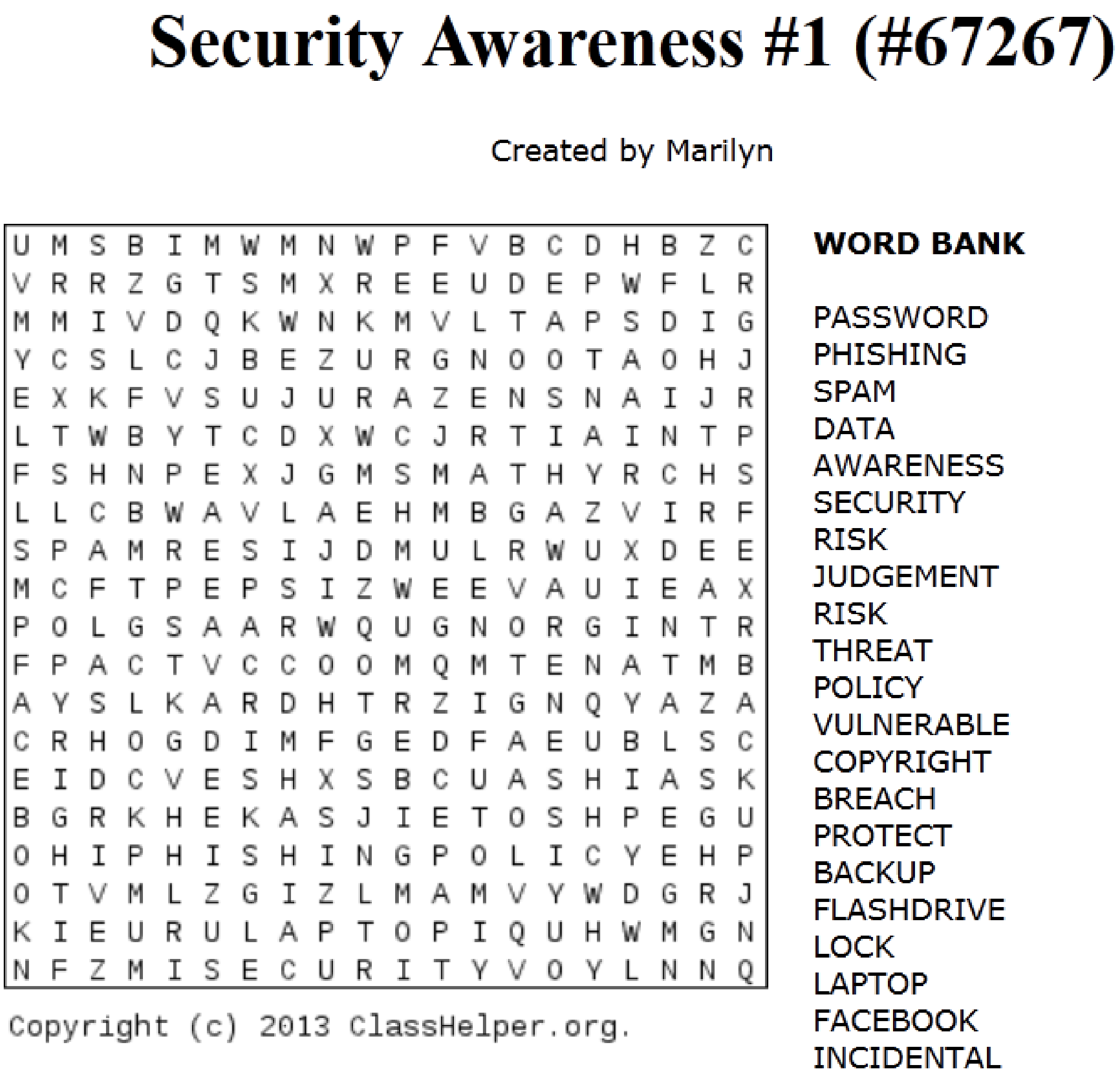
INTRANET
A network (inernal internet) belonging to an organization accessible only by the organizations employees or others with authorization. An intranet's website looks and acts just like any other web sites, but is protected from unauthorized access by a firewall.

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.



Security Awareness #1 (#67267)

Created by Marilyn

U	M	S	B	I	M	W	M	N	W	P	F	V	B	C	D	H	B	Z	C
V	R	R	Z	G	T	S	M	X	R	E	E	U	D	E	P	W	F	L	R
M	M	I	V	D	Q	K	W	N	K	M	V	L	T	A	P	S	D	I	G
Y	C	S	L	C	J	B	E	Z	U	R	G	N	O	O	T	A	O	H	J
E	X	K	F	V	S	U	J	U	R	A	Z	E	N	S	N	A	I	J	R
L	T	W	B	Y	T	C	D	X	W	C	J	R	T	I	A	I	N	T	P
F	S	H	N	P	E	X	J	G	M	S	M	A	T	H	Y	R	C	H	S
L	L	C	B	W	A	V	L	A	E	H	M	B	G	A	Z	V	I	R	F
S	P	A	M	R	E	S	I	J	D	M	U	L	R	W	U	X	D	E	E
M	C	F	T	P	E	P	S	I	Z	W	E	E	V	A	U	I	E	A	X
P	O	L	G	S	A	A	R	W	Q	U	G	N	O	R	G	I	N	T	R
F	P	A	C	T	V	C	C	O	O	M	Q	M	T	E	N	A	T	M	B
A	Y	S	L	K	A	R	D	H	T	R	Z	I	G	N	Q	Y	A	Z	A
C	R	H	O	G	D	I	M	F	G	E	D	F	A	E	U	B	L	S	C
E	I	D	C	V	E	S	H	X	S	B	C	U	A	S	H	I	A	S	K
B	G	R	K	H	E	K	A	S	J	I	E	T	O	S	H	P	E	G	U
O	H	I	P	H	I	S	H	I	N	G	P	O	L	I	C	Y	E	H	P
O	T	V	M	L	Z	G	I	Z	L	M	A	M	V	Y	W	D	G	R	J
K	I	E	U	R	U	L	A	P	T	O	P	I	Q	U	H	W	M	G	N
N	F	Z	M	I	S	E	C	U	R	I	T	Y	V	O	Y	L	N	N	Q

WORD BANK

PASSWORD
PHISHING
SPAM
DATA
AWARENESS
SECURITY
RISK
JUDGEMENT
RISK
THREAT
POLICY
VULNERABLE
COPYRIGHT
BREACH
PROTECT
BACKUP
FLASHDRIVE
LOCK
LAPTOP
FACEBOOK
INCIDENTAL

classhelper.org

Word Jumble Puzzle #1

Unscramble each word below. Unscramble the highlighted letters to form the final word in the puzzle.

rsapwdso	🟨□□□□🟨□□
laidfnconeit	🟨□□□□□□□□□□□
sirvu	□🟨□□□
ssaaweenr	□□□🟨□□□□□
tindeyti fhtet	□□□□□□□🟨■□🟨□□🟨
npsihhgi	□□□□□□□🟨

"Protected by law"

□□□□□□□□□

Word Jumble Puzzle #2

Unscramble each word below. Unscramble the highlighted letters to form the final word in the puzzle.

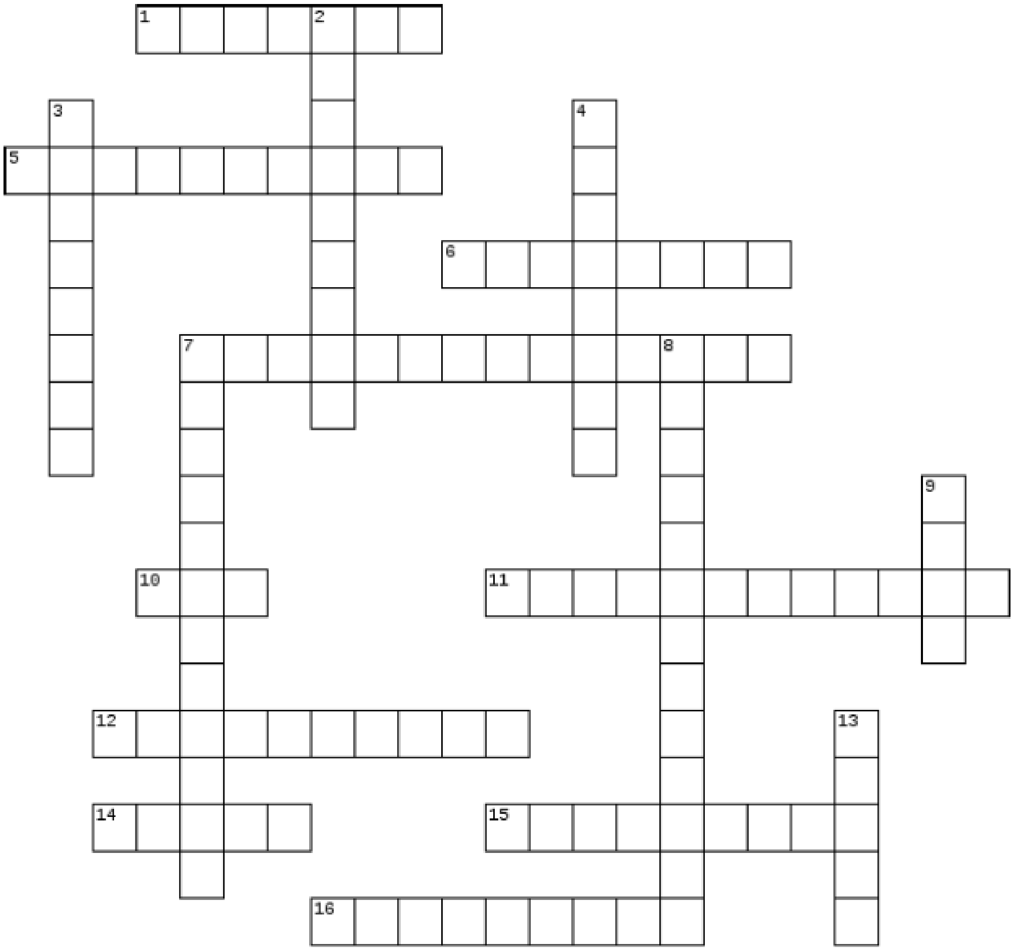
pucksab	□□□□🟨□🟨
ritvainus	🟨□□🟨□🟨□□□
nneettri	□□🟨□□🟨□□
petnoycrin	🟨□🟨□□□□□□□
remawal	□□🟨□□□🟨
dealfitcoini	□□🟨□□🟨□□□□□□

"Know your department's rule"
(two words)

□□□□□□□□□□■□□□

Security Awareness (#2717733)

Created by Marilyn



Across Clues

1. We should have no expectatio of this with respect to SHSU information technology resources
5. The process of transforming information using an algorithm to make it unreadable.
6. Looks like an official e-mail and may contain links to infected websites.
7. The rules that regulate how we manage and protect sensitive information (2 words)
10. All users must sign this acknowledging they have read and understand policy.
11. The category of information that is required by law to be protected.
12. A private combination of words to use for logging into a computer system.
14. A malicious program that can replicate itself &
15. Knowledge and attitude posessed regarding the protection of information.
16. These laws must not be violated by distribuing/downloading protected works.

Down Clues

2. Software that is used to detect, delete and/or neutralize computer-based viruses.
3. A global system interconnecting computers and computer networks.
4. A string of characters that serves as authentication of a person's identity.
7. Using direct observation techniques to get information (2 words)
8. The fraudulent acquisition and use of a person's private identifying information (2 words)
9. Junk e-mail
13. Personal use of information must not result in direct _______ to SHSU.

Answer sheet for crossword puzzle

Answers Across	Answers Down
1. Privacy 5. Encryption 6. Phishing 7. Security Policy 10. NDA 11. Confidential 12. Passphrase 14. Virus 15. Awareness 16. Copyright	2. Antivirus 3. Internet 4. Password 7. Shoulder Surf 8. Identity Theft 9. Spam 13. Costs

Answers for word jumble #1

Password
Confidential
Virus
Awareness
Identity theft
Phishing

Final Word: Copyright

Answers for word jumble #2

Backups
Antivirus
Internet
Encryption
Malware
Confidential

Final Word: Incidental Use

secdoku

S					Y	💻	U	T
💻		U			R	Y		
Y			💻				E	
C			U	💻				I
		S					💻	
	💻		S	Y	I			E
R		💻			U			S
		E	R		💻	C		
	U		I		C		R	💻

Letters to use: U Y T R S I E C

Fill the grid so that all nine rows across, all nine columns down, and all nine 3x3 boxes contain the letters U Y T R S I E C each used only once.

Hint: the correct solution will spell a word diagonally.

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

Acceptable Use Policy: IT-03

PURPOSE:

The computing resources at Sam Houston State University support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the SHSU community. Users of these services and facilities have access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is important to behave in a responsible, ethical, and legal manner.

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. If an individual is found to be in violation of the Acceptable Use Policy, the University will take disciplinary action, up to and including suspension or termination of employment. Individuals are also subject to federal, state and local laws governing interactions that occur on SHSU information technology resources.

This document establishes specific requirements for the use of all computing and network resources at Sam Houston State University. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202) and TSUS Rules and Regulations; Chapter III, Paragraph 19)

SCOPE:

The SHSU Acceptable Use policy applies equally to all individuals utilizing SHSU information technology resources (e.g., employees, faculty, students, alumni, agents, consultants, contractors, volunteers, vendors, temps, etc.).

Information technology resources include 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.

RIGHTS AND RESPONSIBILITIES:

As members of the University community, users are provided with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. There is a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether the user is a University employee or a matriculated student), and of protection from abuse and intrusion by others sharing these resources.

In turn, users are responsible for knowing the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. Users 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.

Users are representatives of the SHSU community, and are expected to respect the University's good name in electronic dealings with those outside the University.

PRIVACY:

All users of state networks and systems should keep in mind that all usage of information technology resources can be recorded and is the property of SHSU. Such information is subject to the Texas Public Information Act and the laws applicable to state records retention. Employees have no right to privacy with regard to use of state-owned resources. SHSU management has the ability and right to view employees' usage patterns and take action to assure that university resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on SHSU information technology resources that are owned, leased, administered, or otherwise under the custody and control of SHSU are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 1 TAC §§202 (Information Security Standards).

ACCEPTABLE USE:

The SHSU network exists to support research, education, and administrative activities by providing access to computing resources and the opportunity for collaborative work. Primary use of the SHSU network must be consistent with this purpose.

Access to the SHSU network from any device must adhere to all the same policies that apply to use from within SHSU facilities.

1. Users may use only SHSU information technology resources for which they are authorized.
2. Users are individually responsible for appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware, and are accountable to the University for all use of such resources.

Authorized users of Sam Houston State University resources may not enable unauthorized users to access the network. The university is bound by its contractual and license agreements respecting certain third-party resources; users must comply with all such agreements when using SHSU information technology resources.

3. Users should secure resources against unauthorized use or access to include SHSU accounts, passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
4. Users must report shareware or freeware that is installed on SHSU-owned equipment unless it is on the approved software list. When software is installed, it must be reported to the IT@Sam Service Desk via email.
5. Users must not attempt to access SHSU information technology resources without appropriate authorization by the system owner or administrator.

RESTRICTIONS:

All individuals are accountable for their actions relating to SHSU information technology resources. Direct violations include the following:

1. Interfering or altering 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. Excessive use for personal purposes, meaning use that exceeds incidental use as determined by supervisor; or,
   e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.
2. Allowing family members or other non-authorized persons to access SHSU information technology resources.
3. Using the SHSU information technology resources for private financial gain or personal benefit. Users are not permitted to run a private business on any SHSU information technology resources. Commercial activity is permitted but only for business done on behalf of SHSU or its organizations.
4. Activities that would jeopardize the University's tax-exempt status.
5. Using SHSU information technology resources for political gain.
6. Using SHSU information technology resources to threaten or harass others in violation of the Texas State University System *Rules and Regulations, Chapter V, Paragraphs 2.4* or *4.51*.
7. Intentionally accessing, creating, storing, or transmitting illegal material.
8. Not reporting any weaknesses in SHSU information technology resources security or any incidents of possible misuse or violation of this agreement by contacting the Information Security Officer.

9. Attempting to access any data or programs contained on SHSU information technology resources for which authorization has not been given.
10. Making unauthorized copies of copyrighted material.
11. Degrading the performance of SHSU information technology services; depriving an authorized SHSU user access to an SHSU information technology resource; obtaining extra information technology resources beyond those allocated; or circumventing SHSU security measures.
12. Downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, SHSU users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on SHSU information technology services.
13. Engaging in acts against the aims and purposes of SHSU as specified in its governing documents or in rules, regulations, and procedures as adopted by SHSU and the Texas State University System.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2015

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

Technology Security Training Policy: IT-13

PURPOSE:

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This will be accomplished with a combination of general computer security awareness training and targeted product-specific training. The philosophy of protection and specific security instructions needs to be taught to and re-enforced with technology users. The security awareness and training information needs to be continuously upgraded and reinforced.

The purpose of the Technology Security Training Policy is to describe the requirements that ensure each user of SHSU information technology resources receives adequate training on technology security issues. Additionally, state law requires that institutions of higher education provide an ongoing information security awareness education program for all users of state-owned information resources (Texas Administrative Code (TAC) §202).

SCOPE:

The SHSU Technology Security Training policy applies equally to all employees.

POLICY STATEMENT:

1. All employees must attend the SHSU Security Awareness Training within 30 days of initially being granted access to SHSU information technology resources, or per request of the data owner or supervisor.

2. Annually, all employees must complete the SHSU Security Awareness training and pass the associated examination.

3. Annually, all employees must sign a non-disclosure agreement per IT-16 Non-Disclosure Agreement Policy stating they have read and understand SHSU requirements regarding IT@Sam policies and procedures.

4. IT@Sam must prepare, maintain, and distribute an Information Security User Guide that concisely describes SHSU information security policies and procedures.
5. IT@Sam must develop and maintain a communication plan that will communicate security awareness to the SHSU user community.

DEFINITIONS:

Information Security User Guide: Describes the requirements that ensure each person has the knowledge to protect SHSU information technology resources, protect themselves and comply with applicable laws.

Non-Disclosure Agreement: Formal acknowledgement that all employees must sign acknowledging they have read and understand SHSU requirements regarding computer security policies and procedures. This agreement becomes permanent record and will be renewed annually.

Security Awareness Training: Annual training required by Texas Administrative Code §202 to re-familiarize users with the SHSU policies, their responsibility to protect SHSU resources and to behave in a responsible, ethical and legal manner.

Texas Administrative Code (TAC) §202): State law that outlines mandatory user security practices, specifically security awareness training and non-disclosure agreements.

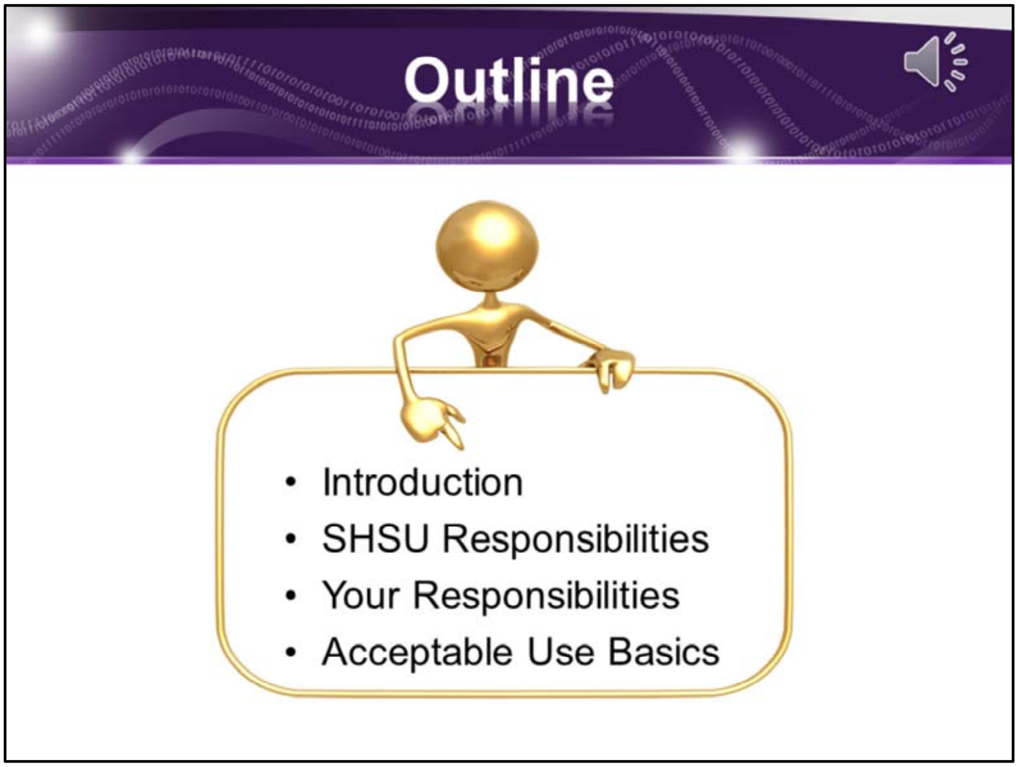
Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by:	Mark C. Adams, VP for Information Technology, November 30, 2014
Approved by:	President's Cabinet, June 27, 2011
Next Review:	November 1, 2017

Sam Houston State University

Security Awareness Training



Outline

- Introduction
- SHSU Responsibilities
- Your Responsibilities
- Acceptable Use Basics

Welcome to SHSUs Security Awareness Training. This video was prepared to educate individuals on the basic responsibilities needed to continue utilizing State of Texas information technology resources, and to ensure each person has the knowledge to protect those resources and themselves.

This program applies equally to all individuals granted access privileges to any SHSU information technology resource.

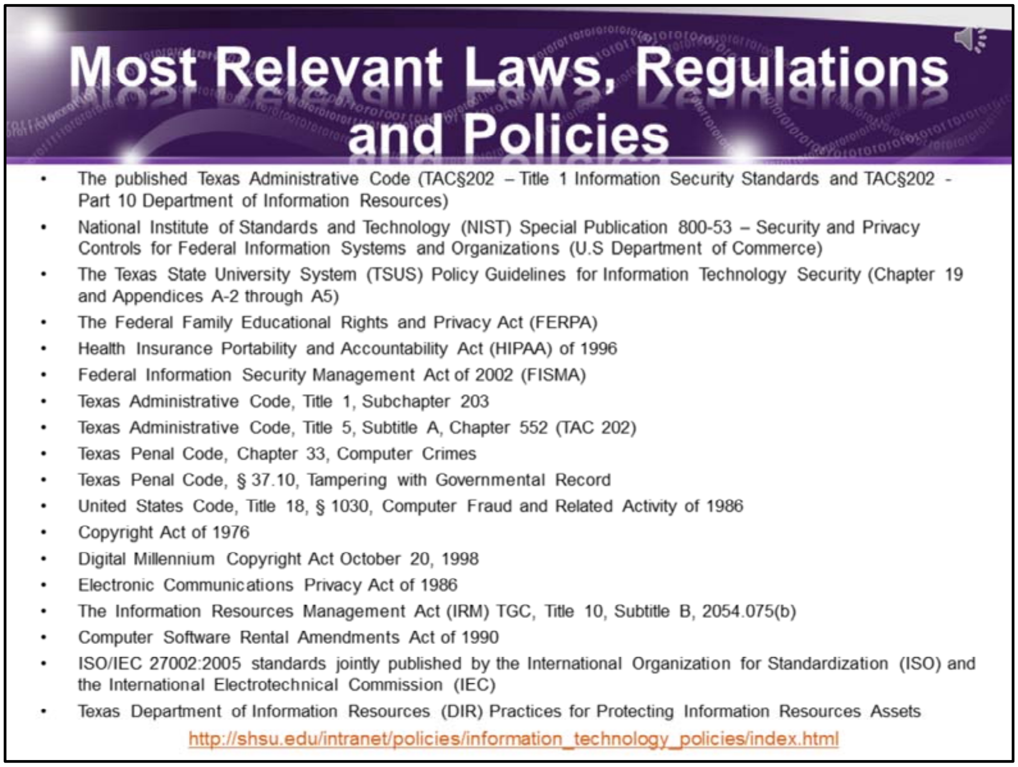
The items we will cover today are:

An Introduction to the laws and policies that govern our security program and where to find them.

The responsibilities of SHSU relating to information security training and education.

Your responsibilities as a user of SHSU information technology resources.

And finally, a review of the acceptable use basics you need to know to be a responsible employee of SHSU.



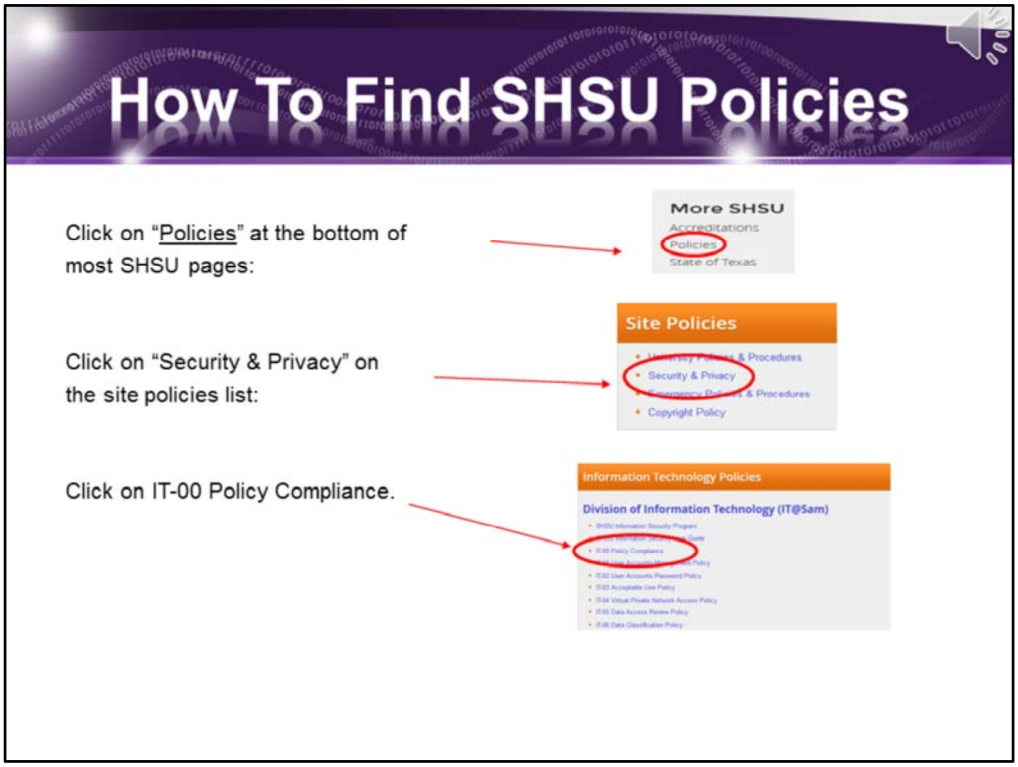
Most Relevant Laws, Regulations and Policies

- The published Texas Administrative Code (TAC§202 – Title 1 Information Security Standards and TAC§202 - Part 10 Department of Information Resources)
- National Institute of Standards and Technology (NIST) Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations (U.S Department of Commerce)
- The Texas State University System (TSUS) Policy Guidelines for Information Technology Security (Chapter 19 and Appendices A-2 through A5)
- 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
- 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

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

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 here.

Don't let this lengthy list frighten you, they are listed in IT-00, our Compliance Policy for you to refer to any time you need. I'll show you how to find the Information Security Policies.



How To Find SHSU Policies

Click on "Policies" at the bottom of most SHSU pages:

Click on "Security & Privacy" on the site policies list:

Click on IT-00 Policy Compliance.

More SHSU
Accreditations
Policies
State of Texas
Site Policies
University Policies & Procedures
Security & Privacy
Emergency Policies & Procedures
Copyright Policy
Information Technology Policies
Division of Information Technology (IT@Sam)
SHSU Information Security Program
IT-00 Policy Compliance
IT-02 User Accounts Password Policy
IT-03 Acceptable Use Policy
IT-04 Virtual Private Network Access Policy
IT-05 Data Access Review Policy
IT-06 Data Classification Policy

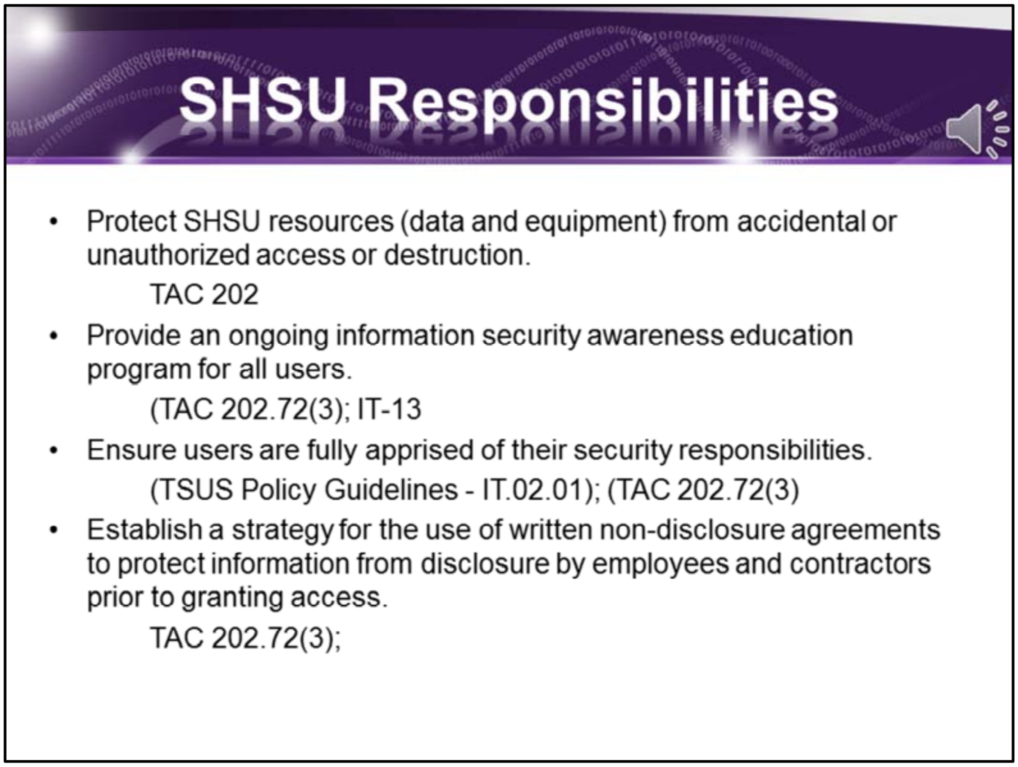
SHSU security policies are derived from the previous list laws, regulations and policies, particularly The Texas Administrative Code (known as TAC 202).
Under the guidance of the Department of Information Resources, these laws were transformed into thirty IT policies and categorized by subject matter
so it s easier to find a particular policy. Our job is to keep the policies up to date and aligned with state and federal laws and guidelines.

At the bottom of most of the SHSU web pages you will find a frame with important links to internal and external sites.

To access all IT policies, click on "Policies" at the bottom of the page.

click on "Security & Privacy" on the site policies list.

Click on the policy that you are interested in (e.g. IT-00) If you have any problems, please contact the service desk.



SHSU Responsibilities

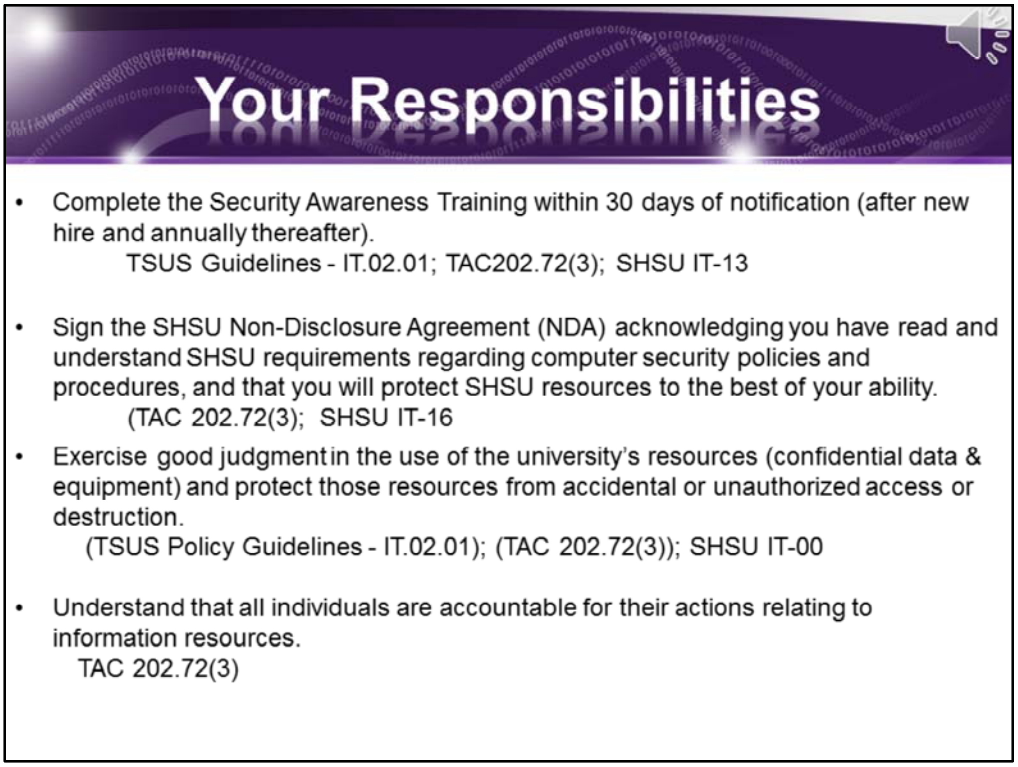
- Protect SHSU resources (data and equipment) from accidental or unauthorized access or destruction.
  TAC 202
- Provide an ongoing information security awareness education program for all users.
  (TAC 202.72(3); IT-13
- Ensure users are fully apprised of their security responsibilities.
  (TSUS Policy Guidelines - IT.02.01); (TAC 202.72(3)
- Establish a strategy for the use of written non-disclosure agreements to protect information from disclosure by employees and contractors prior to granting access.
  TAC 202.72(3);

It's not only important for you to understand YOUR responsibilities, but it helps to understand ours. We are here to help you.

The following responsibilities are directly from the Texas Administrative Code, TSUS Policy Guidelines, and our own Security Policies identified under each paragraph.

We must protect SHSU resources from accidental or unauthorized access or destruction.
Provide an ongoing information security awareness education program for all users.
Ensure users are full apprised of their security responsibilities.
And establish a strategy for the use of written non-disclosure agreements.

Both the security awareness program and non-disclosure agreements will be administered through the Talent management system.

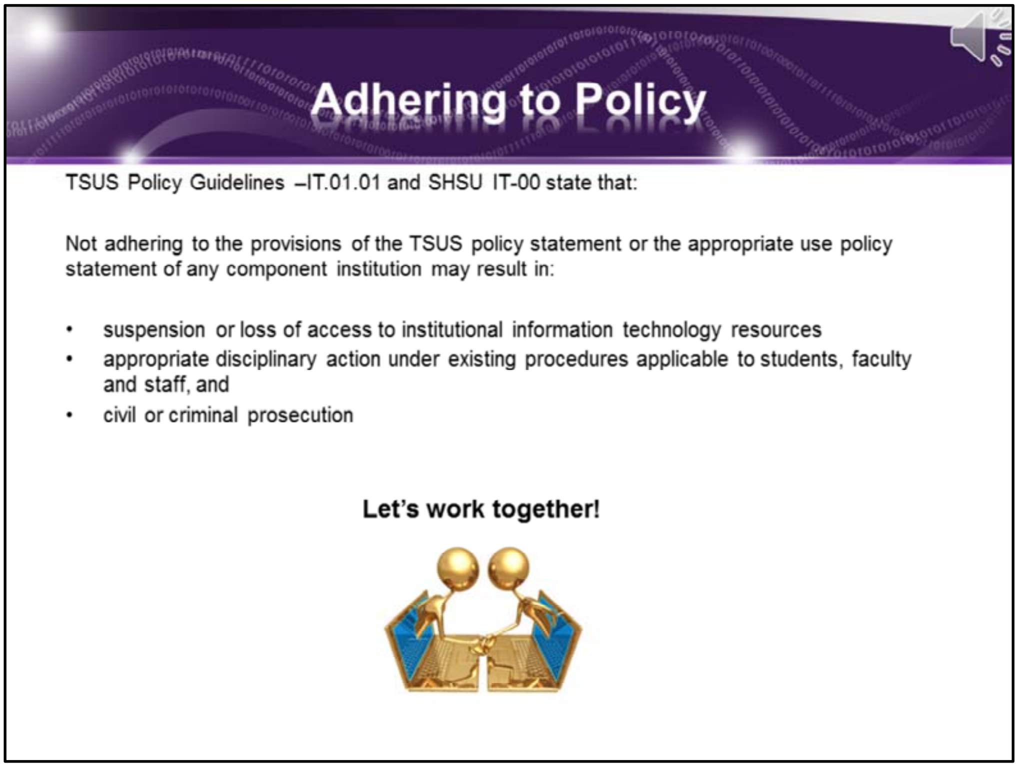


Your Responsibilities

- Complete the Security Awareness Training within 30 days of notification (after new hire and annually thereafter).
  TSUS Guidelines - IT.02.01; TAC202.72(3); SHSU IT-13
- Sign the SHSU Non-Disclosure Agreement (NDA) acknowledging you have read and understand SHSU requirements regarding computer security policies and procedures, and that you will protect SHSU resources to the best of your ability.
  (TAC 202.72(3); SHSU IT-16
- Exercise good judgment in the use of the university's resources (confidential data & equipment) and protect those resources from accidental or unauthorized access or destruction.
  (TSUS Policy Guidelines - IT.02.01); (TAC 202.72(3)); SHSU IT-00
- Understand that all individuals are accountable for their actions relating to information resources.
  TAC 202.72(3)

The following responsibilities, your responsibilities, as directed by the identified Texas Administrative Code, TSUS Policy Guidelines, and our own Security Policies under each paragraph.

You must
Complete the security awareness training, through talent management, within 30 days of notification and annually thereafter.
Sign the Non-disclosure agreement acknowledging you understand SHSU requirements and will protect SHSU resources to the best of your ability.
Exercise good judgment in the use of the university's resources. We will get a little more in depth further into this presentation.
Understand that you are accountable for your actions relating to information resources.



Adhering to Policy

TSUS Policy Guidelines –IT.01.01 and SHSU IT-00 state that:

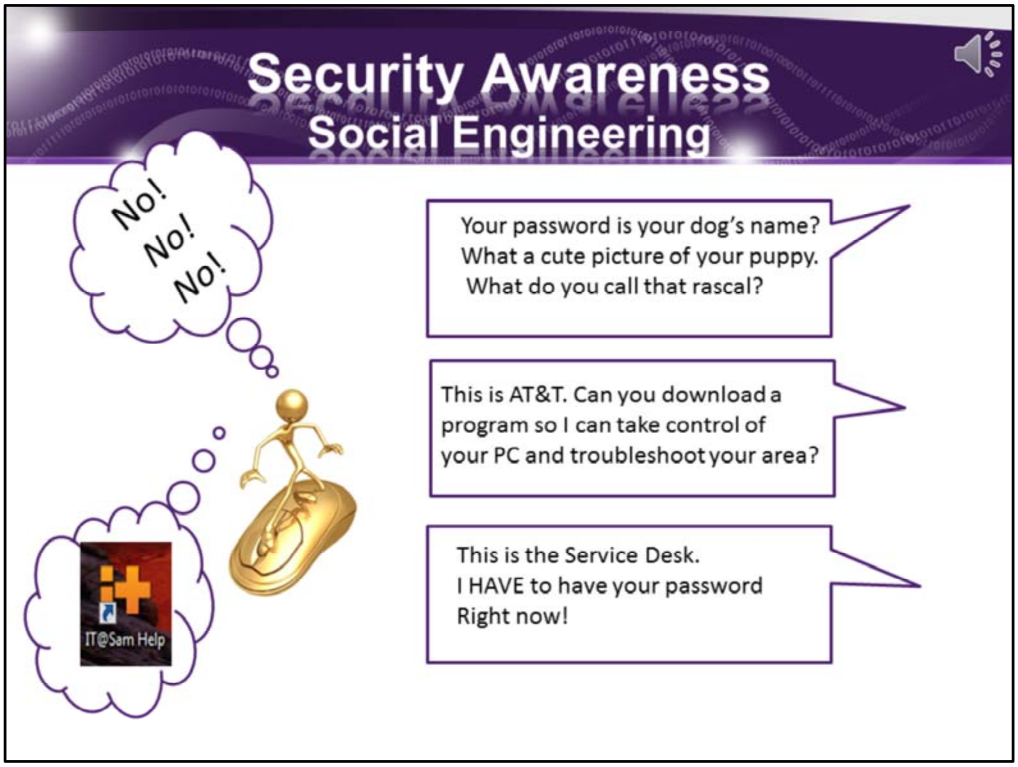
Not adhering to the provisions of the TSUS policy statement or the appropriate use policy statement of any component institution may result in:

- 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

Let’s work together!

Our guiding authority, Texas State University System’s guidelines, requires that you understand the consequences of not adhering to the information security policies. Depending on the severity of your actions and whether a law has been broken, consequences could range from loss of access to the network, suspension, to civil or criminal prosecution.

Let’s work together to fulfill our responsibilities and protect our information resources.



Security Awareness
Social Engineering

No!
No!
No!
IT@Sam Help

Your password is your dog's name? What a cute picture of your puppy. What do you call that rascal?

This is AT&T. Can you download a program so I can take control of your PC and troubleshoot your area?

This is the Service Desk.
I HAVE to have your password
Right now!

Here at SHSU, security is a top priority, which is why we want to inform you about the policies and standards that will protect both you and the university, as well as keep us in compliance with laws and regulations. You help play a big part in information security.

Not only does the law recognize that the #1 reason for data breaches is the Human; but so does the criminal. Criminals target individuals as well as companies. And the best way to get through a company's defenses is through the individual. This is usually accomplished through social engineering, which is psychological manipulation of people into performing actions or divulging confidential information. They trick you into thinking they are your bank, your help desk, a co-worker or your internet provider and convince you to disclose information you normally wouldn't.   If they are asking for information they shouldn't have, or create a sense of urgency or persistence, be wary, they are probably trying to manipulate you.

For example, someone calls you identifying themselves as an AT&T technician and ask you to go out to the internet and download a small program that will help them troubleshoot wireless problems in the area.   Be suspicious. If you are uncomfortable with their request, tell them that you are very busy and ask for a call back number and name to get with later. This will usually make them just hang up.   You can also direct them to the service desk.

Security Awareness

Other Social Engineering

Shoulder Surfer

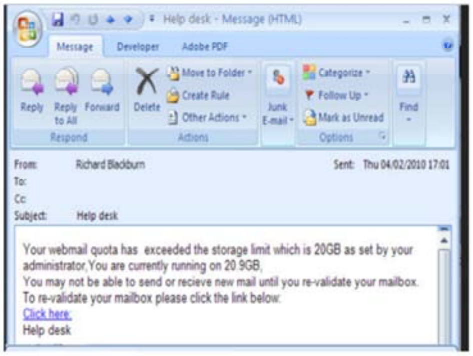
Lock your screen every time you step away

Very interesting!
Darn! It's locked.... grumble...
Out to Lunch
+ L

All reasonable precautions to prevent data compromise should be taken when using pcs, laptops, tablets, smart phones, or other campus computing resources. Shield your screen from passive viewing (like “shoulder surfing” which is someone viewing your screen from over your shoulder, and password protect your screen whenever you step away). If you walk away from your computer leaving it logged in and exposed, remember anyone sitting down to use it will have access to anything YOU would have access to – Banner, your payroll information on MySam, etc. Lock your screen by either using the Ctl+Alt+Del keys and Choosing ‘lock this computer’ or easier still… hold down the Windows key on the keyboard and press the letter L. Your programs will continue to run behind the locked screen, but safe from roaming eyes.

Security Awareness
Phishing

Don’t get hooked….



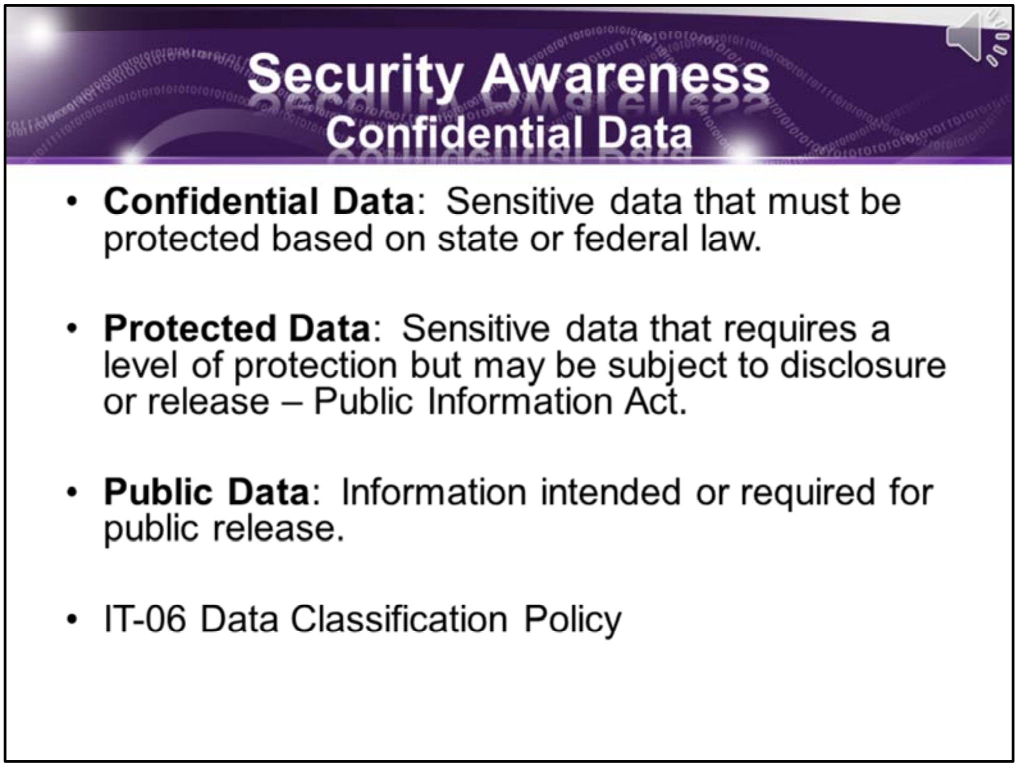
From: Richard Blackburn Sent: Thu 04/02/2010 17:01
To:
Cc:
Subject: Help desk

Your webmail quota has exceeded the storage limit which is 20GB as set by your administrator,You are currently running on 20.9GB,
You may not be able to send or recieve new mail until you re-validate your mailbox.
To re-validate your mailbox please click the link below:
Click here:
Help desk

One of the most common examples of social engineering is phishing. Phishing is the activity of deceiving an individual through email. Usually an email is received from someone you think you trust, with a link to click on that leads to a fake site that requests confidential information. They could be asking for account numbers, personal information, or your log on credentials (username and password) for your bank, home account, SHSU account, etc. Know that SHSU will never send you an email requesting your logon credentials. If you receive one that appears to be from IT@Sam requesting your credentials, do not comply, it is most definitely a phishing scam. If you think an email COULD be from your bank or another trusted source, do not use the link in the email. Go to your browsers list of favorites where you always access that site and log in through it. If there is correspondence from them that is legit, it will be on the REAL page as well.

Be suspicious of any email that threatens to shut down your email account or bank account, any email that looks like it comes from a reputable organization but has bad grammar or misspellings, or one that creates a sense of urgency by requesting Immediate Action. Before clicking on a link, hover your mouse over the link to display the real website and compare to the legitimate website. Don’t click on attachments unless you are expecting them – it could be carrying a virus that will infect your computer without you knowing. If you are suspicious, delete it.

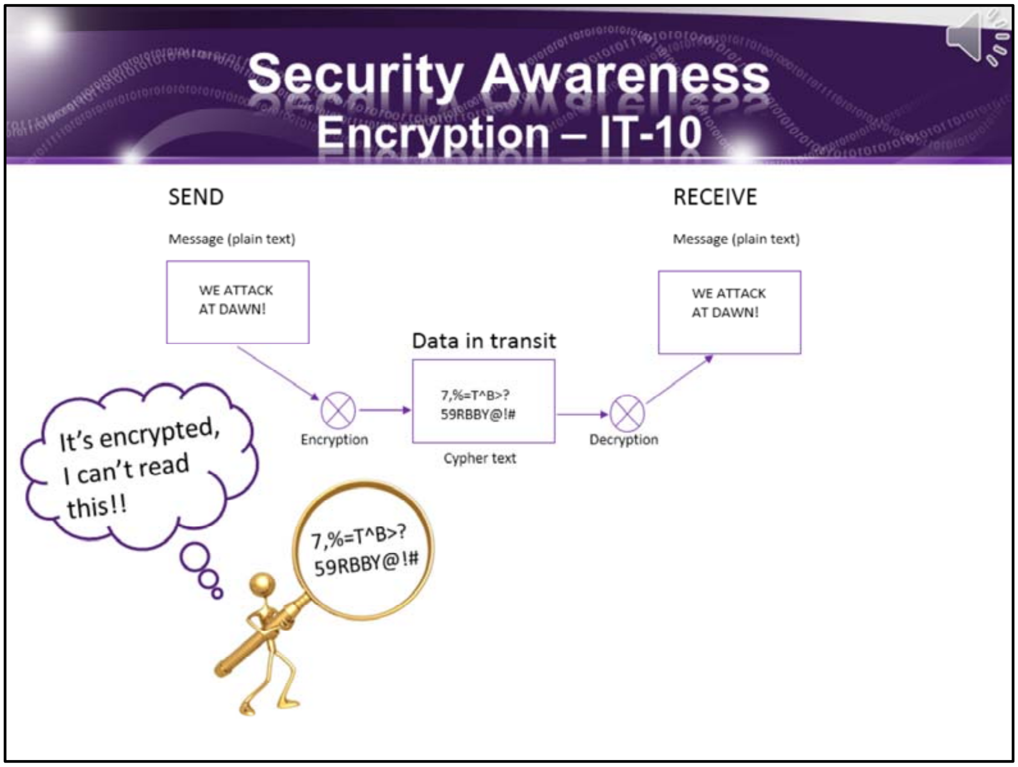
The information you give can end up compromising your account and allow them to gain access to confidential data, bank account information, medical history, or identity theft; or they can gain total control of your computer to hack others or distribute SPAM. If you think they have nothing to gain from accessing your account, remember, whatever you have access to – they will have access to because of Single Sign on. They could open IE and access your MySam portal which has your personal information and payroll information. They would also have access to anything in Banner that you can access, which includes students personal information and grades.



Security Awareness
Confidential Data

- **Confidential Data**: Sensitive data that must be protected based on state or federal law.
- **Protected Data**: Sensitive data that requires a level of protection but may be subject to disclosure or release – Public Information Act.
- **Public Data**: Information intended or required for public release.
- IT-06 Data Classification Policy

Always understand the confidential level of the information that you work with. If you don’t know, ask your supervisor. A general description of the different types of information and examples are outlined in IT-06 Data Classification Policy.



Security Awareness

Encryption – IT-10

SEND

Message (plain text)

WE ATTACK
AT DAWN!

Encryption

Data in transit

7,%=T^B>?
59RBBY@!#

Cypher text

Decryption

RECEIVE

Message (plain text)

WE ATTACK
AT DAWN!

Take care when copying, saving or transporting confidential data. Never attach a document that contains confidential data to an email unless you have encrypted that file.

Unencrypted documents are called 'clear text'. This means if a hacker gains access to your unencrypted document it is read easily in clear text. Encryption 'scrambles' the content of your data with mathematical algorithms to ensure hackers cannot read it, this is called 'cypher text'.   The data stays scrambled while it is in transit, so it remains safe.

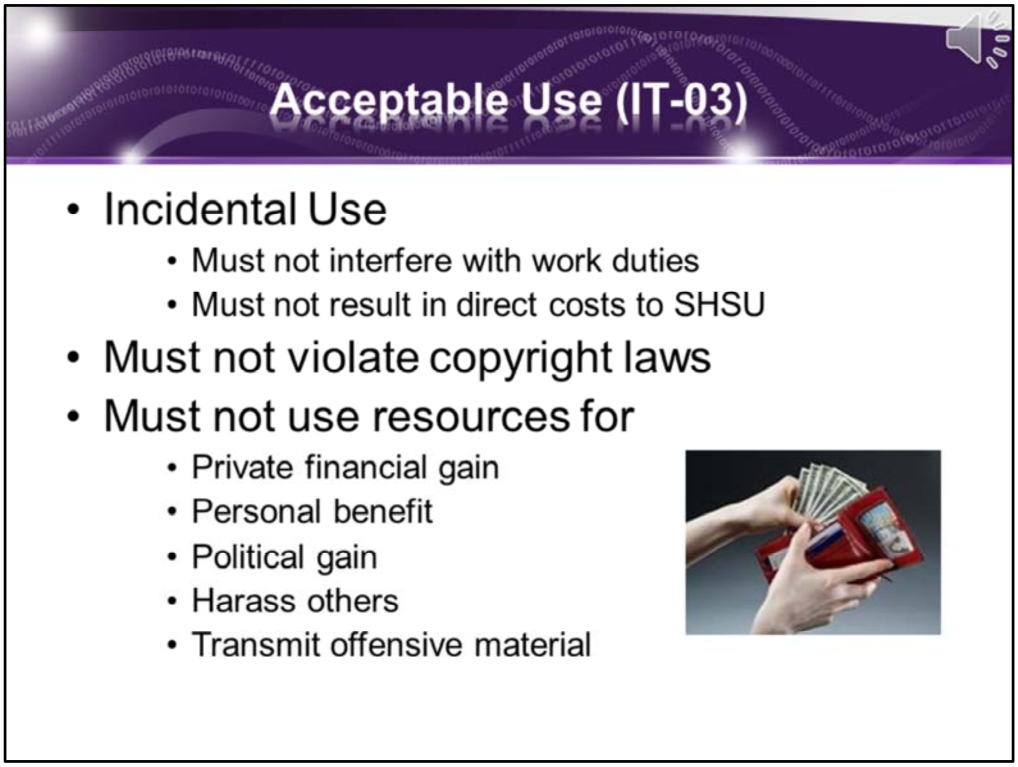
When it reaches it's destination, decrypting will put it back to it's original form.

If you store confidential data on a laptop or tablet, it must be protected with encryption. Please contact the service desk to obtain help with encrypting files and devices.

Never store confidential data on public 'cloud' drives like skydrive, google docs, etc. There is no way we can be assured of the security around that confidential data.

Security Awareness
Web Browsing

When using your web browser to browse the internet, there is always the risk of going to an infected website. . There is no simple way to tell if a website is malicious or has been compromised. Criminals will use unprotected, unpatched browsers to gain control of your computer.   SHSU IT@Sam’s team patches the university’s servers and PCs every month when Microsoft releases them, which remediates any known vulnerabilities, to give you the best possible protection.   We ask that you use good judgment when browsing the web. If something looks wrong, it probably is.



Acceptable Use (IT-03)

- Incidental Use
  - Must not interfere with work duties
  - Must not result in direct costs to SHSU
- Must not violate copyright laws
- Must not use resources for
  - Private financial gain
  - Personal benefit
  - Political gain
  - Harass others
  - Transmit offensive material

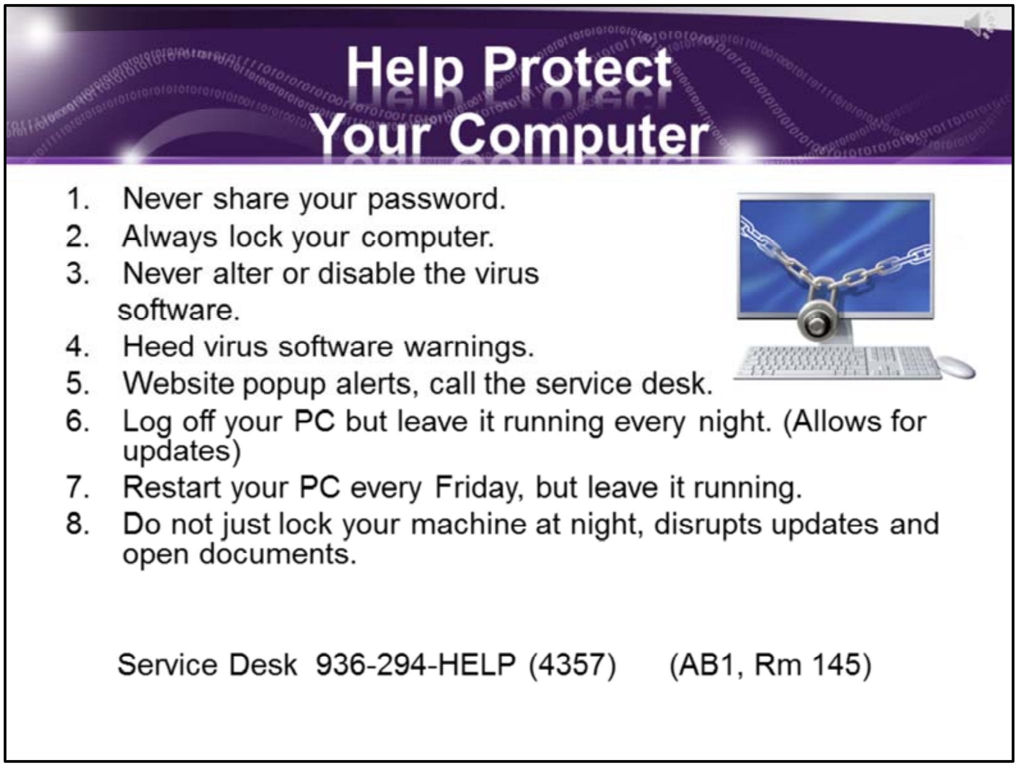
The state of Texas, TSUS system and SHSU allow for “incidental use” while on campus. Incidental use would be “personal use” like checking your personal email, facebook, twitter, etc.
While there is no definitive timeframe for how much time you spend on incidental use, you must check with your individual supervisor to find out if your department has a restriction as to the amount of personal use you are allowed. **Excessive use is determined by your supervisor or department head.**

The laws that govern incidental use:
Personal use must not interfere with the normal performance of an employees work duties.
-must not result in direct costs to SHSU – color printing, etc.

-users must not violate copyright laws – so no downloading protected works such as copyrighted movies or music.

-users must not use the SHSU resources for
private financial gain,
personal benefit (such as running a personal business or trading stocks from SHSU.
or political gain.
-users must not
threaten or harass others or
intentionally access, create, store or transmit material that may be offensive, indecent or obscene.

Again, use good judgment.



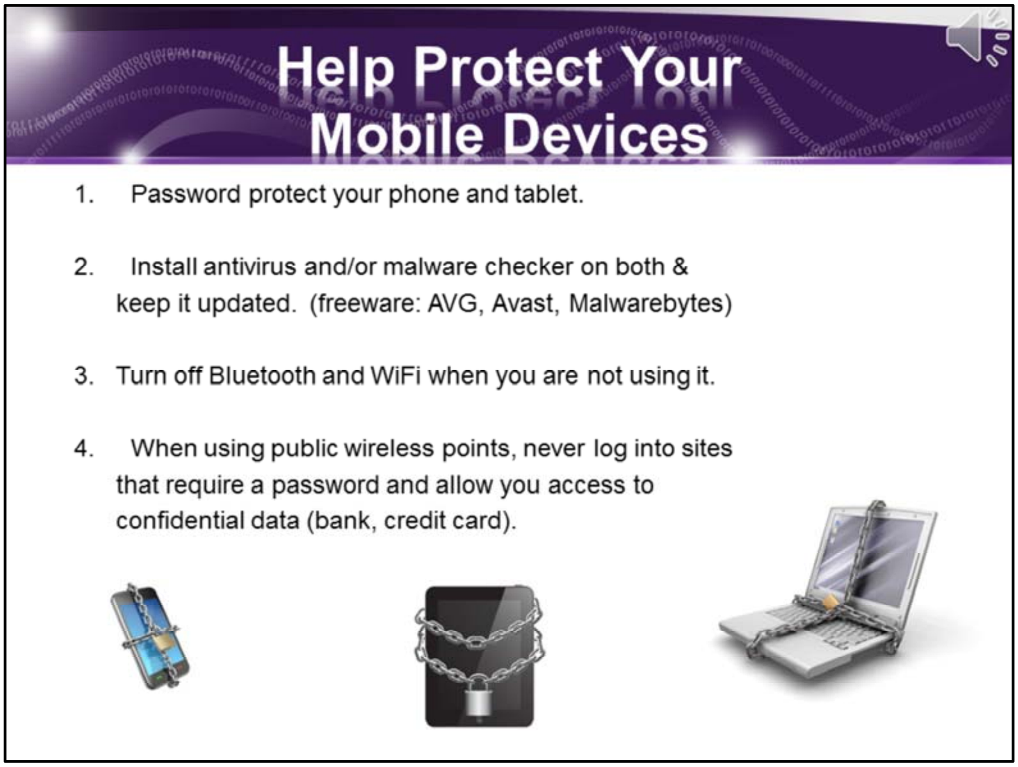
Help Protect Your Computer

1. Never share your password.
2. Always lock your computer.
3. Never alter or disable the virus software.
4. Heed virus software warnings.
5. Website popup alerts, call the service desk.
6. Log off your PC but leave it running every night. (Allows for updates)
7. Restart your PC every Friday, but leave it running.
8. Do not just lock your machine at night, disrupts updates and open documents.

Service Desk 936-294-HELP (4357) (AB1, Rm 145)

NOT RECORDED YET:

There are steps you can take to help us protect your computer.
1. NEVER share your password with anyone. Remember it is the keys to the kingdom!
2. Always lock your computer when you are away – Never leave it unattended. “Windows” key +L.
3. Never alter or disable the virus protection software. If there’s an abundance of pop-ups or messages– there’s a reason. Contact the service desk for help.
4. If your virus software warns that there is a problem that cannot be fixed, call the service desk immediately.
5. If you get a pop-up from a website alerting you of any problems, call the service desk immediately. It could be that you have already been infected with a virus or malware.
6. Log off, and leave your computer up and running, every evening so IT@Sam can push the necessary updates to protect your computer. And restart it on Friday evening or first thing Monday morning.
7. Restart our PC.
8. If you just lock your computer leaving yourself logged in overnight, updates might be disrupted. Or worse, there are updates that will restart your computer and open documents could be lost or corrupted.



Help Protect Your Mobile Devices

1. Password protect your phone and tablet.

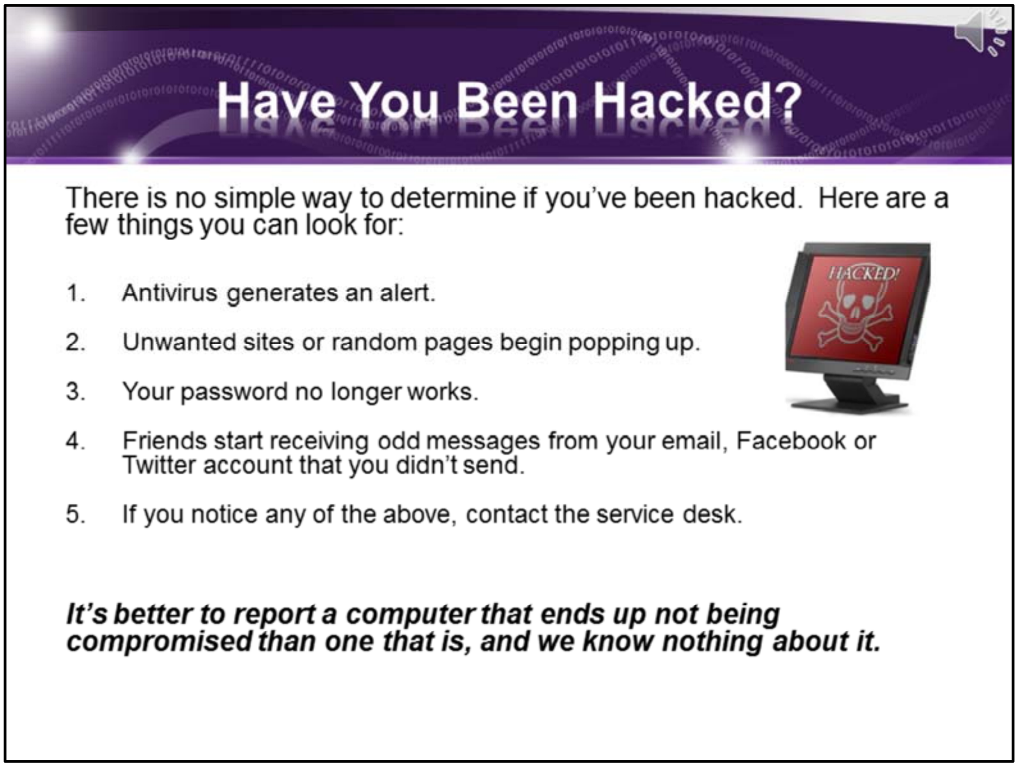
2. Install antivirus and/or malware checker on both & keep it updated. (freeware: AVG, Avast, Malwarebytes)

3. Turn off Bluetooth and WiFi when you are not using it.

4. When using public wireless points, never log into sites that require a password and allow you access to confidential data (bank, credit card).

Protect your Mobile devices both at work and at home. Think of your phone or tablet as a mini-PC – and treat it as such.

1. Password protect your phone or tablet.
2. Install an antivirus or malware checker on your phone and tablet and keep them updated – there are plenty of free apps out there that are great. There's no need to pay for them.
Eg AVG, Avast, Malwarebytes.
3. Turn off Bluetooth and wifi when you are not using it, this will help keep hackers from attacking you when you least expect it.
4. When working on public wireless points, never log in to sites that require a password to allow you access to confidential data like your bank or credit card company. A hacker could be 'sniffing' the open network and pick up your logon credentials – to later log into your account.



Have You Been Hacked?

There is no simple way to determine if you've been hacked. Here are a few things you can look for:

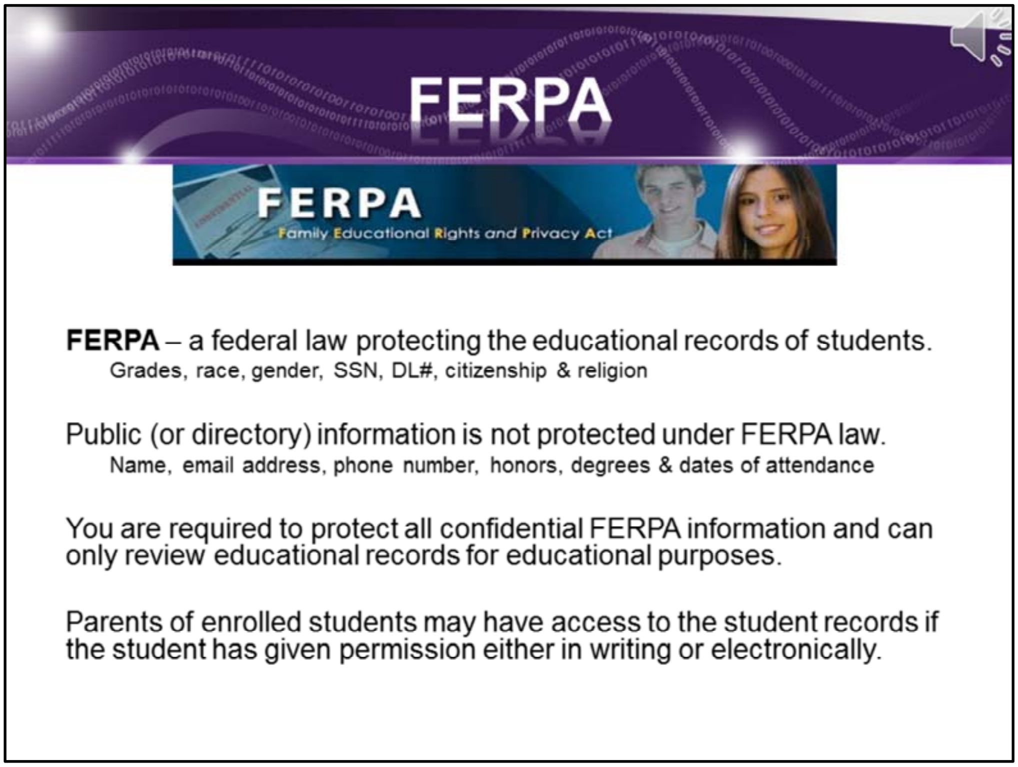
1. Antivirus generates an alert.
2. Unwanted sites or random pages begin popping up.
3. Your password no longer works.
4. Friends start receiving odd messages from your email, Facebook or Twitter account that you didn't send.
5. If you notice any of the above, contact the service desk.

It's better to report a computer that ends up not being compromised than one that is, and we know nothing about it.

Unfortunately, there is no simple way to determine if you've been hacked. Here are a few things you can look for:
Be suspicious

1. If your antivirus generates an alert, this mean there's something unusual going on and it needs to be investigated.
2. If your browser is taking you to unwanted sites or random pages begin popping up, there is a problem.
3. Your password no longer works. Hacker could've already gained your credentials, logged on and changed it. Go thru your 'password reset' process to regain control of your account.
4. Friends start receiving messages from your email, facebook or twitter account that you know you didn't send. Your account has been hacked. Reset your passwords.
5. If you notice any of the above or need help, contact the service desk.

It's better to report a pc that ends up not being compromised than one that is and we know nothing about it.



FERPA

FERPA
Family Educational Rights and Privacy Act

FERPA – a federal law protecting the educational records of students.
Grades, race, gender, SSN, DL#, citizenship & religion

Public (or directory) information is not protected under FERPA law.
Name, email address, phone number, honors, degrees & dates of attendance

You are required to protect all confidential FERPA information and can only review educational records for educational purposes.

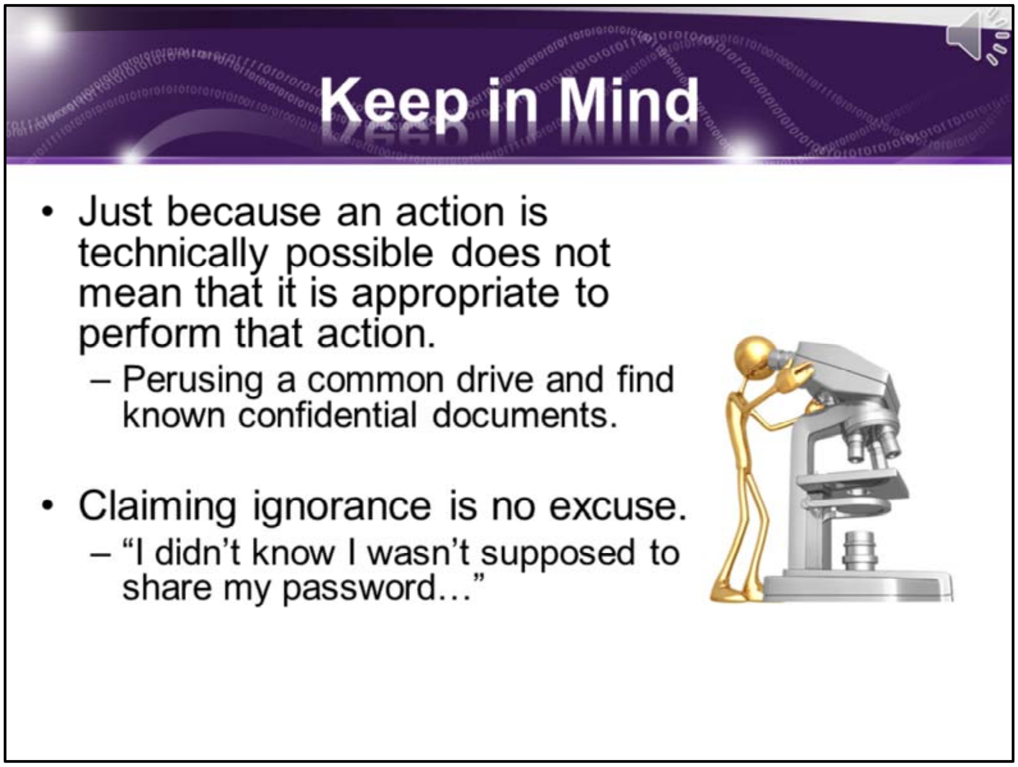
Parents of enrolled students may have access to the student records if the student has given permission either in writing or electronically.

Every university employee is tasked with adhering to FERPA laws
FERPA – a federal law protecting the educational records of students. (eg, Grades, race, gender, ssn, DL#, citizenship and religion)

Public (or directory) information is not protected under the FERPA law, such as: Name, email address, phone number, honors and degrees, and dates of attendance

You are required to protect all confidential FERPA information. This includes discussing the educational records of students with other staff and faculty. You can only review educational records for educational purposes.
An example of educational purposes might be that a student asks you to write a letter of recommendation for him or her. This is a legitimate reason to need to review their educational records.
But if a student applies for a job in your department, you may not review his or her educational records to make that decision – this is not a legitimate educational purpose.

Parents of enrolled students may have access to the student records if the student has given permission either in writing or electronically.



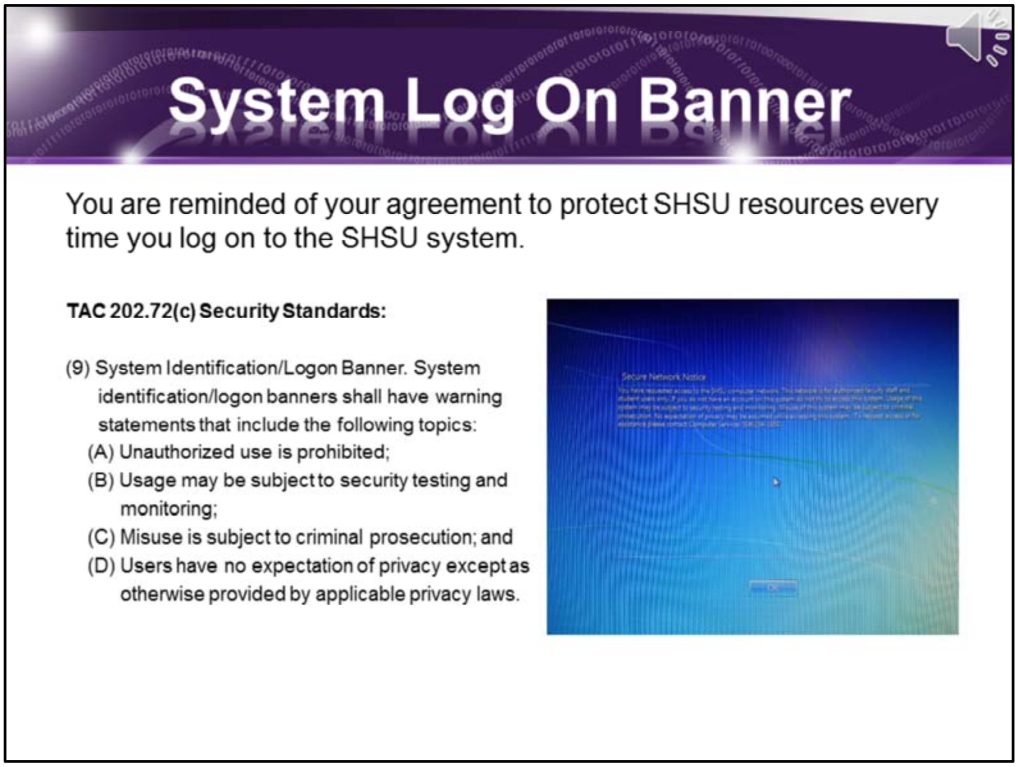
Keep in Mind

- Just because an action is technically possible does not mean that it is appropriate to perform that action.
  - Perusing a common drive and find known confidential documents.
- Claiming ignorance is no excuse.
  - "I didn't know I wasn't supposed to share my password…"

There are 2 things to keep in mind:
Just because an action is technically possible does not mean that it is appropriate to perform that action.

For instance, you are in the T: drive- your departmental drive. You come upon a folder named "Performance Evaluations" and open it. Inside you find your co-workers performance evals, filled out with grades and private comments. You know this is information you aren't supposed to have access to. Use good judgment and ethics. Immediately get out of the folder and contact the service desk. Tell them you ran across a folder that you feel you probably shouldn't have access to. They will fix the permissions on that folder.

Claiming ignorance is no excuse. Such as "I didn't know i wasn't supposed to share my password". You are exposed to these basics at New Hire Training and annually through Talent Management. In addition, October is Cyber Security Awareness Month where we reinforce the basics of information security campus wide for the entire month.



System Log On Banner

You are reminded of your agreement to protect SHSU resources every time you log on to the SHSU system.

TAC 202.72(c) Security Standards:

(9) System Identification/Logon Banner. System identification/logon banners shall have warning statements that include the following topics:
- (A) Unauthorized use is prohibited;
- (B) Usage may be subject to security testing and monitoring;
- (C) Misuse is subject to criminal prosecution; and
- (D) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

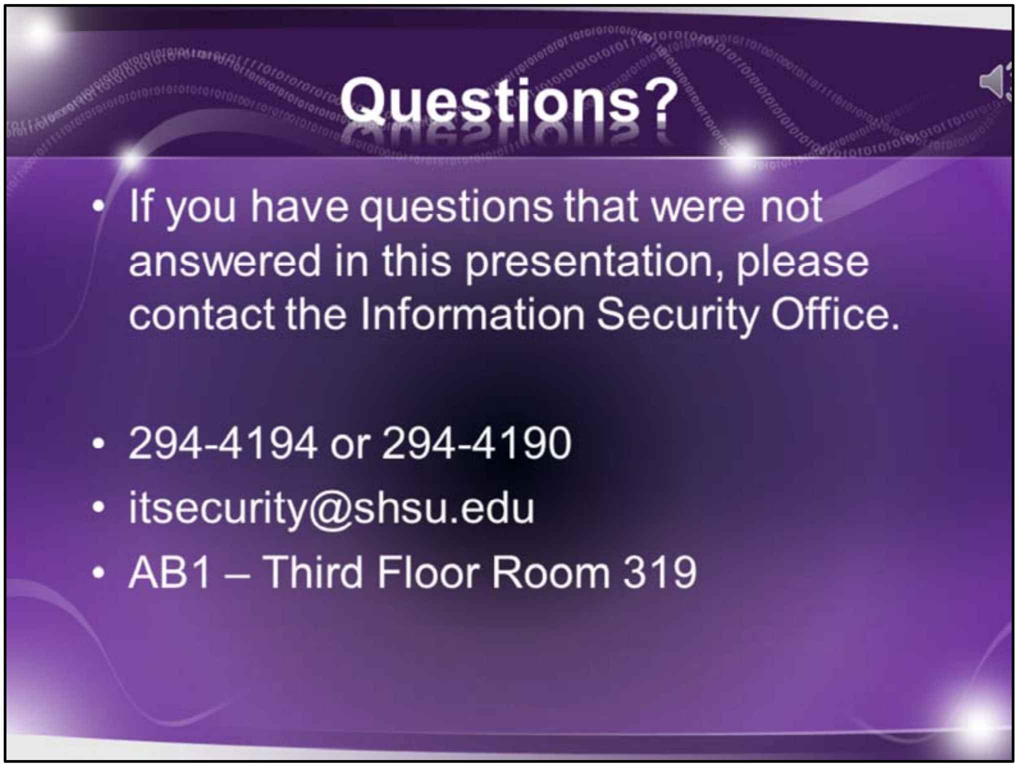
Secure Network Notice

[illegible]

Every time you log into the SHSU network, you are reminded through a System Log On Banner called “Secure network Notice“ of your responsibility to protect SHSU resources.

TAC 202 clearly points out that we are required to remind you every time you log on that:

Unauthorized use is prohibited
Usage may be subject to testing and monitoring
Misuse is subject to criminial prosecution
And users have no expectation of privacy.



Questions?

- If you have questions that were not answered in this presentation, please contact the Information Security Office.
- 294-4194 or 294-4190
- itsecurity@shsu.edu
- AB1 – Third Floor Room 319

This concludes your annual basic security awareness training.

If you have access to special data such as PCI, HIPAA or CJ data, you will have additional training to attend through Talent management.

If you have any questions, please contact the Information Security Office.

To exit this training
please click on the
“X” at the top right corner
of this window.

“To exit this training, please click on the “X” at the top right corner of this window.”

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

User Accounts Password Policy: IT-02

PURPOSE:

All user accounts will be protected by passwords that are both strong and confidential. Users will protect the security of those passwords by managing passwords according to the account holders responsibilities specified in this policy.

System and Application Administrators will ensure account passwords are secured using industry best practices.

SCOPE:

The SHSU User Accounts Password policy applies equally to all individuals granted access privileges to any Sam Houston State University information technology resources.

POLICY:

Users are responsible for what is accessed, downloaded, or created under their credentials regardless of intent. An unauthorized person can cause loss of information confidentiality, integrity and availability that may result in liability, loss of trust, or embarrassment to SHSU.

Account holders responsibilities:

1. Must create a strong password and protect it.
2. Password must have a minimum length of six (6) alphanumeric characters.
3. Password must contain a mix of upper case, lower case and numeric characters or special characters (!@#%^&*+=?/~';:,<>|\).
4. Passwords must not be easy to guess, for instance, they should not include part of your social security number, your birth date, your nickname, etc.
5. Passwords must not be easily accessible to others (e.g. posted on monitors, under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. SHSU username and password should not be used for external services (e.g. LinkedIn, Facebook or Twitter).

9. Users should never share their password with anyone, including family, supervisors, co-workers and IT@Sam personnel.
10. Users will be required to change passwords at least once per 180 days.
11. If you know or suspect that your account has been compromised, change your password immediately and contact IT@Sam Service Desk for further guidance and assistance.
12. It IT@Sam suspects your account has been compromised, your account will be deactivated and you will be contacted immediately.

Any individuals responsible for managing passwords must:

1. Prevent or take steps to reduce the exposure of any clear text, unencrypted account passwords that SHSU applications, systems, or other services have received for purposes of authentication.
2. Never request that passwords be transmitted unencrypted. Of particular importance is that passwords never be sent via email.
3. Never circumvent this password policy for the sake of ease of use.
4. Coordinate with IT@Sam regarding password procedures.

Detailed information and instructions for password management can be found on the SHSU website in the New Employee Technology Orientation training booklet. http://www.shsu.edu/~ucs_www/docs/TrainingBooklet.pdf

DEFINITIONS:

Application Administrator: The individual responsible for the support, troubleshooting, administration, design, and implementation of a specific application.

Compromised Account: The unauthorized use of a computer account by someone other than the account owner.

Encrypted: The conversion of data into a form, called cipher text that cannot be easily understood by unauthorized people. Encryption is achieved using Windows native Bit Locker or other available software.

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.

Password: A string of characters input by a system user to substantiate their identity, authority, and access rights to the computer system that they wish to use.

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

Unauthorized person: A person who has not been given official permission or approval to access SHSU systems.

Unencrypted: Information or data that has not been converted into code that would prevent unauthorized access.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, VP for Information Technology, May 20, 2011
Approved by: President's Cabinet, June 27, 2011
Reviewed and Approved by: Mark Adams, VP for Information Technology, September 30, 2013
Reviewed and Approved by: Mark Adams, VP for Information Technology, January 30, 2015
Reviewed and Approved by: Mark Adams, VP for Information Technology, August 17, 2015
Reviewed and Approved by: Mark Adams, VP for Information Technology, September 1, 2016
Next Review: November 1, 2018

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

Data Backup and Recovery Policy: IT-11

PURPOSE:

The purpose of the Data Backup Policy is to manage and secure backup and restoration processes and the media employed within these processes; prevent the loss of data in the case of administrator error or corruption of data, system failure, or disaster; and ensure periodic restoration of data to confirm it is recoverable in a useable form.

SCOPE:

The SHSU Data Backup policy applies to any data owner, data custodian, system administrator and IT@Sam staff that installs, operates or maintains SHSU information technology resources.

POLICY STATEMENT:

1. IT@Sam System Administrators are responsible for backing up IT@Sam-managed servers and are required to implement a tested and auditable process to facilitate recovery from data loss.
2. 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 and will be the responsibility of the data owner.
3. SHSU IT@Sam System Administrators will perform daily data backups of all IT@Sam managed servers containing critical data for the purposes listed above.
    a. Individual drives (e.g. S drive) and email will be retained for 14 days.
    b. All other data, such as Enterprise Application Data (e.g. Banner and Oracle data) and shared storage backups (e.g. T drive) will be retained for 60 days.
    c. Policy exceptions to the stated retention times will be at the discretion of the President utilizing the IT@Sam Policy Exception Form .
    d. SHSU will not be responsible for data stored on non-SHSU cloud storage systems (e.g. One Drive) and data will be subject to that vendors' retention terms of service.
4. Determining which data and information is deemed ‘critical’ (e.g. confidential data and other data considered to be of institutional value) is the responsibility of the Data Owner, per SHSU Data Classification Policy (IT-06). Data identified by the Data Owner as non-critical may be excluded from this policy. Alternative backup schedules and media management may be requested by the data owner commensurate with the criticality of the data and the capabilities of the tools used for data storage.

5. Records retention is the responsibility of the Data Owner. The IT@Sam backups are not to be used to satisfy the retention of records and are not customized for all the varying retention periods.
6. Monthly backup data will be stored at a location that is physically different from the original data source.
7. Verification, through restoration of backed-up data, must be performed on a regular basis as defined by the IT@Sam back-up procedures document for the respective system.
8. Procedures for backing up of critical data and the testing of the procedures must be documented. Such procedures must include at a minimum for each type of data:
    a. A definition of the specific data to be backed up.
    b. The backup method to be used (full backup, incremental backup, differential, mirror, or a combination).
    c. The frequency and time of data backup.
    d. The number of generations of backed up data that are to be maintained (both on site and off site).
    e. The responsible individual(s) for data backup.
    f. The storage site(s) for the backups.
    g. The storage media to be used.
    h. The naming convention for the labels on storage media.
    i. Any requirements concerning the data backup archives.
    j. The data transport modes.
        i. For data transferred during any backup process, end-to-end security of the transmission path must be ensured for confidential data.
    k. The recovery of backed up data.
        i. Processes must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.
    l. The destruction of obsolete backup media as described in SHSU Media Sanitization Policy (IT-15).

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, VP for Information Technology, June 28, 2016
Approved by: President's Cabinet, March 6, 2013
Next Review: November 1, 2018

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

Data Classification Policy: IT-06

PURPOSE:

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All SHSU data, whether electronic or printed, must be classified as Confidential, Protected, or Public. Consistent use of data classification reinforces with users the expected level of protection of SHSU data assets in accordance with SHSU policies.

The purpose of the Data Classification Policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

SCOPE:

The SHSU Data Classification policy applies equally to all Data Owners and Data Custodians.

POLICY STATEMENT:

Data Owners and/or Data Custodians must classify data as follows:

1. Confidential: Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act, FERPA, HIPPA) and other constitutional, statutory, judicial, and legal agreements. Examples of Confidential data may include, but are not limited to:

    a. Personally identifiable information such as a name in combination with Social Security Number (SSN) and/or financial account numbers
    b. Student education records such as posting student identifiers and grades
    c. Intellectual property such as copyrights, patents and trade secrets
    d. Medical records

2. Protected: Sensitive data that may be subject to disclosure or release under the Texas Public Information Act but requires additional levels of protection. Examples of Protected data may include but are not limited to SHSU:

    a. Operational information
    b. Personnel records
    c. Information security procedures
    d. University-related research
    e. SHSU internal communications

3. Public: Information intended or required for public release as described in the Texas Public Information Act.

DEFINITIONS:

Confidential Data: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

Data Classification: Classifying data according to their category of Confidential, Protected or Public.

Data Custodian: The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Protected Data: Sensitive data that requires a level of protection but may be subject to disclosure or release – Public Information Act.

Public Data: Information intended or required for public release.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 30, 2015
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2016

STUDENT PRIVACY INFORMATION

HOME (/) / DEPARTMENTS (/DEPT/) / REGISTRAR (/DEPT/REGISTRAR/) / STUDENTS (/DEPT/REGISTRAR/STUDENTS/)

Family Education Rights and Privacy Act (F.E.R.P.A.) –

The Family Educational Rights and Privacy Act of 1974, as amended, is a federal law which provides that colleges and universities will maintain the confidentiality of student education records. This law also affords students certain rights with respect to their education records.

The law basically says that no one outside the institution shall have access to students' education records nor will the institution disclose any information from those records without the written consent of the student. There are exceptions, of course, so that certain personnel within the institution may see the records, including persons in an emergency in order to protect the health or safety of students or other persons.

Additionally, under FERPA, students have the right to:

- Inspect and review their education records
- Seek to amend their education records
- Have some control over the disclosure of information from their education records (Buckley Amendment)
- File a complaint for an alleged violation of FERPA rights

FERPA law provides that an institution of higher education shall state what information in a student education record is to be considered Directory Information which may be released without prior student consent. Under FERPA, Sam Houston State University has established the following as directory information:

- Name
- Local/Home/E-mail Addresses
- Major/Minor
- Local/Home Telephone Numbers
- Degrees, Diplomas, Certificates and Date of Award
- Honors and Awards
- Classification
- Extracurricular Activities
- Birth Date and Place of Birth
- Names and Addresses of Parents/Legal Guardians
- Weight, Height, and Related Information of Athletic Team Member

The above directory information will be available for release to the general public. However, the Buckley Amendment under FERPA, states that each student has the right to inform Sam Houston State University that any or all of the above information is not to be released. Sam Houston State University will honor the student's request to restrict the release of "Directory Information" as listed.

A student may restrict the release of directory information by submitting the Buckley Amendment Form (found on this page under the Forms link) to the Registrar's Office located on the 3rd floor of the Estill Building. Forms must be submitted to the Registrar's Office prior to the

Office of the Registrar

- Home (/dept/registrar/index.html)
- Transcripts and Student Records
- Registration
- Texas Success Initiative (TSI) (/dept/registrar/texas-success-initiative/index.html)
- Student Resources
- Graduation
- Parent Resources (/dept/registrar/parents/index.
- Faculty and Staff
- About Us

Important Dates and Calendars

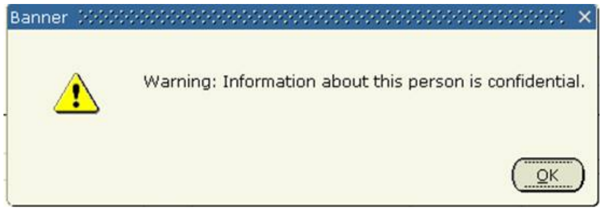
- Advance Registration (/dept/registrar/calendars/adva registration.html)
- Academic Calendar (/dept/registrar/calendars/acac calendar.html)
- Registration/Payment Dates (/dept/registrar/students/regist dates.html)
- Add/Drop Deadlines (/dept/registrar/students/regist dates.html#schedule-changes)
- Resignations, Refunds, and Drop Policies (/dept/registrar/students/regist refunds-drops.html)
- Final Exam Schedule (/dept/registrar/calendars/final exam-schedules.html)

twelfth class day of the fall and spring terms and the fourth class day of the summer term. Additionally, the restriction of information remains on the students' record until the student takes action to remove it. If the student restricts their information, the university campus staff and faculty will view a confidential message on all student records found in our current Banner student information system and **NO** information can be released on that student without the written permission of the student. This includes the restriction of the student's name being listed in the commencement program, the honor's list, and the Dean's/President's list. Release of information contained on a student's academic transcript without the written consent of the person(s) identified on the document is in violation of Sec. 438 Public Law 90-247 (FERPA).

Additional FERPA information regarding our University policies on student rights is available under the Student Guidelines maintained by the Dean of Students (http://www.shsu.edu/~slo_www/). For more information, please visit www.shsu.edu/students/guide/ (http://www.shsu.edu/students/guide/).

REMINDER TO ALL EMPLOYEES

If you see this message when you enter a Student ID into any Banner form,
you cannot release any information on that student:



Warning: Information about this person is confidential.

* Additionally, if you see the word, "Confidential" on the top left-hand corner of any Banner form, you cannot release any information on that student.

It is a violation of FERPA to discuss a student's record with any person without a legitimate education interest. This pertains to discussions on and off the job.

- Removing any document from the office for non-business purposes is in violation of FERPA.
- Releasing confidential student information (non-directory) to another student, University organization, or any person who does not have a legitimate educational interest, or parents of a dependent student, without the student's written authorization is in violation of FERPA.
- Leaving reports or computer screens containing confidential student information in view of others who do not have a legitimate educational interest in the data or leaving your monitor unattended is in violation of FERPA.
- Making personal use of student information is in violation of FERPA.
- Allowing another person to use your computer access code is in violation of FERPA.
- Putting paperwork in trash with a student's information (i.e., social security or grades) is also in violation of FERPA.

Violation of confidentiality and security may lead to appropriate personnel action.

QUESTIONS?

The FERPA campus official at Sam Houston State University is the Registrar. If you have any questions concerning FERPA or what information can or cannot be released, please contact the Registrar's Office. If we cannot answer your question, we will consult the Department of Education.

Registrar's Office
BOX 2029
Huntsville TX 77341

(936)294-1048

Or

Toll free (866) 232-7528 ext 41048

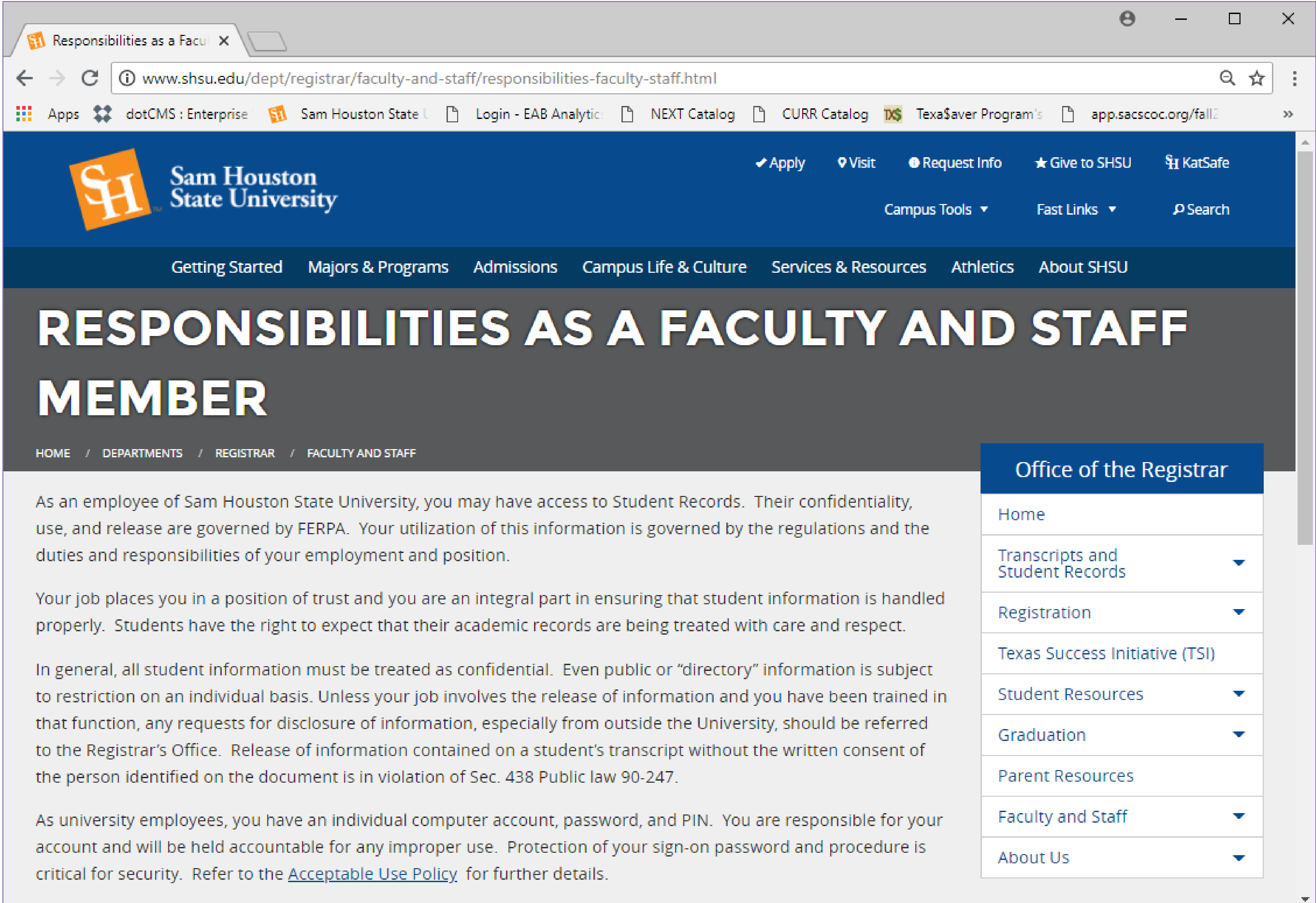
Email at: registrar@shsu.edu (mailto:ask.regstaff@shsu.edu)

Buckley Amendment Release Form +

Responsibilities as a Student Employee +

Parental Access to Children's Education Records +

Parent Page Account Login +



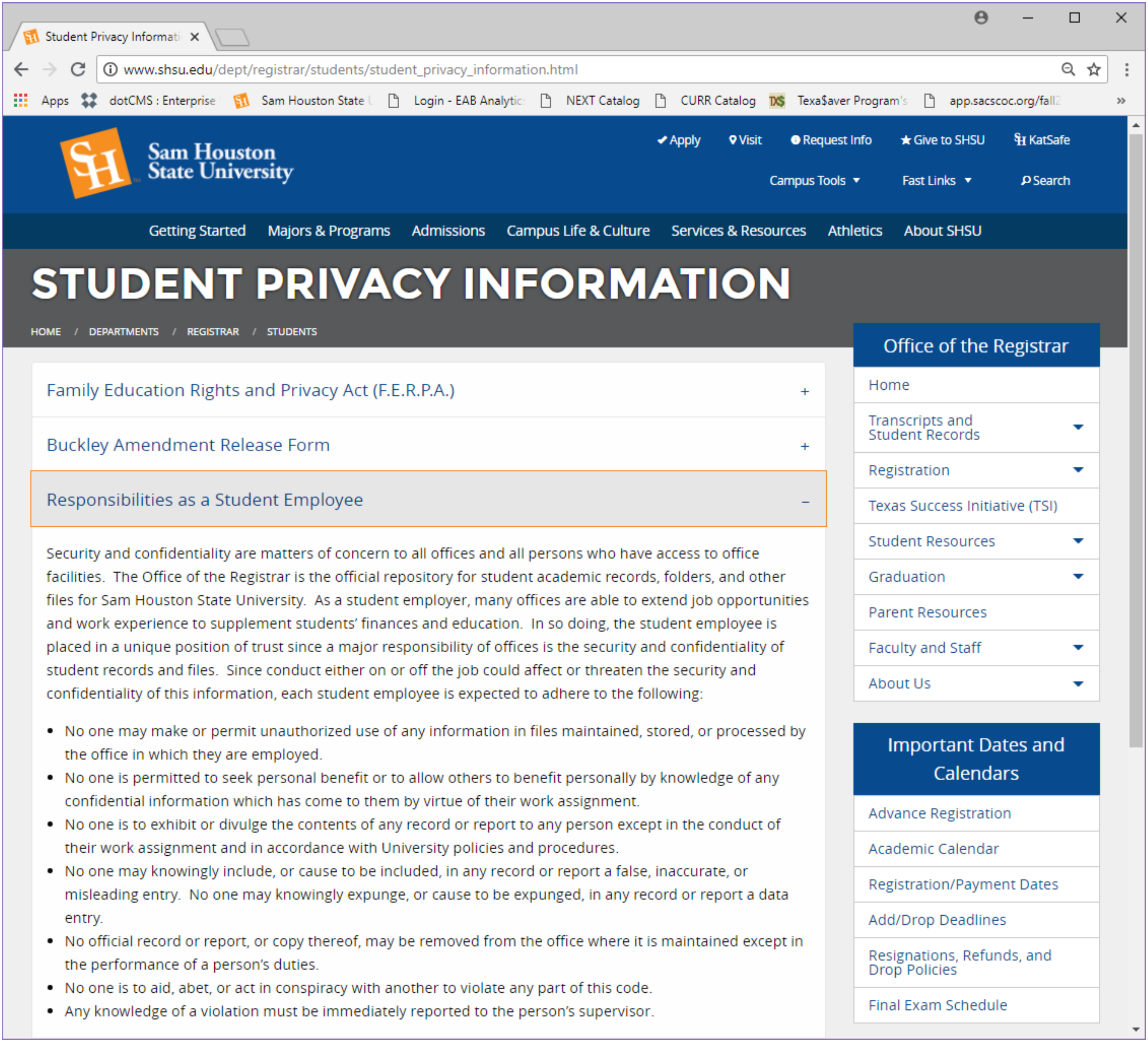
RESPONSIBILITIES AS A FACULTY AND STAFF MEMBER

As an employee of Sam Houston State University, you may have access to Student Records. Their confidentiality, use, and release are governed by FERPA. Your utilization of this information is governed by the regulations and the duties and responsibilities of your employment and position.

Your job places you in a position of trust and you are an integral part in ensuring that student information is handled properly. Students have the right to expect that their academic records are being treated with care and respect.

In general, all student information must be treated as confidential. Even public or "directory" information is subject to restriction on an individual basis. Unless your job involves the release of information and you have been trained in that function, any requests for disclosure of information, especially from outside the University, should be referred to the Registrar's Office. Release of information contained on a student's transcript without the written consent of the person identified on the document is in violation of Sec. 438 Public law 90-247.

As university employees, you have an individual computer account, password, and PIN. You are responsible for your account and will be held accountable for any improper use. Protection of your sign-on password and procedure is critical for security. Refer to the Acceptable Use Policy for further details.



STUDENT PRIVACY INFORMATION

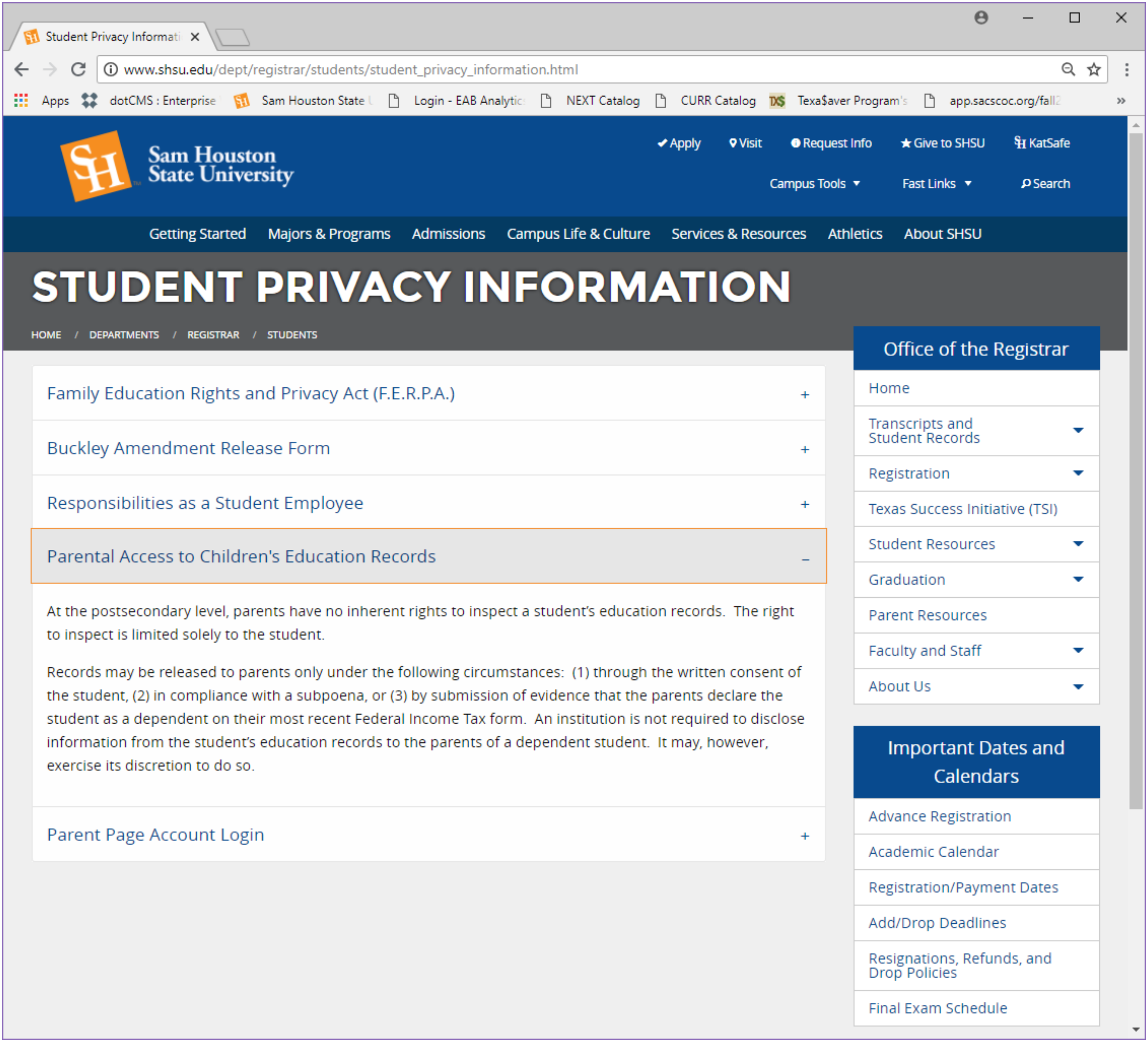
Family Education Rights and Privacy Act (F.E.R.P.A.) +

Buckley Amendment Release Form +

Responsibilities as a Student Employee –

Security and confidentiality are matters of concern to all offices and all persons who have access to office facilities. The Office of the Registrar is the official repository for student academic records, folders, and other files for Sam Houston State University. As a student employer, many offices are able to extend job opportunities and work experience to supplement students' finances and education. In so doing, the student employee is placed in a unique position of trust since a major responsibility of offices is the security and confidentiality of student records and files. Since conduct either on or off the job could affect or threaten the security and confidentiality of this information, each student employee is expected to adhere to the following:

- No one may make or permit unauthorized use of any information in files maintained, stored, or processed by the office in which they are employed.
- No one is permitted to seek personal benefit or to allow others to benefit personally by knowledge of any confidential information which has come to them by virtue of their work assignment.
- No one is to exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and in accordance with University policies and procedures.
- No one may knowingly include, or cause to be included, in any record or report a false, inaccurate, or misleading entry. No one may knowingly expunge, or cause to be expunged, in any record or report a data entry.
- No official record or report, or copy thereof, may be removed from the office where it is maintained except in the performance of a person's duties.
- No one is to aid, abet, or act in conspiracy with another to violate any part of this code.
- Any knowledge of a violation must be immediately reported to the person's supervisor.



STUDENT PRIVACY INFORMATION

Family Education Rights and Privacy Act (F.E.R.P.A.) +

Buckley Amendment Release Form +

Responsibilities as a Student Employee +

Parental Access to Children's Education Records –

At the postsecondary level, parents have no inherent rights to inspect a student's education records. The right to inspect is limited solely to the student.

Records may be released to parents only under the following circumstances: (1) through the written consent of the student, (2) in compliance with a subpoena, or (3) by submission of evidence that the parents declare the student as a dependent on their most recent Federal Income Tax form. An institution is not required to disclose information from the student's education records to the parents of a dependent student. It may, however, exercise its discretion to do so.

Parent Page Account Login +

termination, depending upon the circumstances.

The SHSU Drug Awareness program is a three part program to inform employees about:

1. Health risk involved in the use of illicit drugs and the abuse of alcohol which often result in poor health and premature death.
2. Help available for drug and alcohol counseling, treatment, and rehabilitation that is offered to all SHSU employees.
3. Local sanctions which include fines and/or imprisonment for violation of local, state, or federal drug laws.

SHSU is obligated to uphold laws which prohibit the possession, use, or distribution of controlled substances. Any employee who is found to be in violation of these laws will be dismissed and referred to the appropriate legal authority for prosecution. The SHSU Human Resources Department is the source of information and confidential assistance for any employee who is seeking help for a drug or alcohol related problem. Please contact the Human Resources Department, located in the College of Humanities & Social Sciences Building, Suite 410, phone number (936) 294-1070 if you need additional information about this program.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974

1. Access to Records

Compliance with the Family Education Rights and Privacy Act requires that a university policy be provided to eligible students upon request. (Subpart A Section 99.5) The following information complies with this act. The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records. They are:

(1) The right to inspect and review the students' education records within 45 days of the day the university receives a request for access.

Students should submit to the registrar, dean, head of the department, or other appropriate official, written requests that identify the record(s) they wish to inspect. The university official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the university official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

(2) The right to request amendment of the student's education records that the student believes are inaccurate or misleading.

Students may ask the university to amend a record that they believe is inaccurate or misleading. They should write the university official responsible for the record, clearly identify the part of the record they want changed, and specify why it is inaccurate or misleading.

If the university decides not to amend the record as requested by the student, the university will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedure will be provided to the student when notified of the right to a hearing.

(3) The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.

One exception which permits disclosure without consent is disclosure to school officials with legitimate educational interests. A school official is a person employed by the university in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the university has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

A school official has a legitimate educational interest if the official needs to review an educational record in order to fulfill his or her professional responsibility.

Upon request, the university discloses education records without consent to officials of another school, in which a student seeks or intends to enroll. [Note: FERPA requires an institution to make a reasonable attempt to notify the student of the records request unless the institution states in its annual notification that it intends to forward records on request. The right to file a complaint with the U.S. Department of Education concerning alleged failures by State University to comply with the requirements of FERPA. The name and address of the office that administers FERPA is:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Ave., SW
Washington, DC 20202-4605.

2. Directory Information

Under the terms of the Family Educational Rights and Privacy Act, Sam Houston State University has established the following as directory information: (1) Name, (2) Local/Home Address, (3) Major, (4) Minor, (5) Local/Home Telephone Number, (6) Degrees, Diplomas, and Certificates and Date of Award, (7) Honors and Awards, (8) Classification, (9) Extracurricular Activities, (10) Birthdate and Place of Birth, (11) Names and Addresses of Parents/Legal Guardians, (12) Weight, Height, and Related Information of Athletic Team Member.

The above directory information will be available for release to the general public. However, the act states that each student has the right to inform Sam Houston State University that any or all of the above information is not to be released. Sam Houston State University will honor the student's request to restrict the release of "Directory Information" as listed above, but cannot assume responsibility to contact the student for subsequent permission to release the information. Regardless of the effect upon the student, the institution assumes no liability for honoring the student's instructions to restrict the release of "Directory Information." A student may restrict the release of directory information by submitting the Buckley Amendment Form to the Registrar's Office located on the 3rd floor of the Estill Building (form is available online under the Registrar's Office page). Forms must be submitted to the Registrar's Office prior to the twelfth class day of the fall and spring terms and the fourth class day of the summer term. A student who has restricted the release of personal information will not have his or her name listed in the Dean's List of Academic Honors or the President's Honor Roll, the Commencement Program, and/or Honors list. For more information, please visit www.shsu.edu/ferpa or contact the Registrar's Office.

FIRST YEAR REQUIRED HOUSING AND MEAL PLAN POLICY

All first year students are required to reside in university housing and to purchase a specific meal plan during their freshman year, which will normally include the fall and spring semesters. Anyone signing an academic year housing/meal plan contract will be

Confidentiality of Patient Health Information (PHI)

I. Policy

All staff employed by the Student Health Center (SHC) as well as student workers, interns, and volunteers are to maintain the confidentiality of personal health information (PHI) to which they have access in the course of fulfilling their daily job duties.

II. Definitions

Patient Identifiers-Any demographic information that may identify a specific patient such as name, address, birthdate, phone number, email, social security number, medical records number, account number, license number, and photograph.

Protected Health Information (PHI)-Any health information in the medical record or designated record that was created, used or disclosed in the course of providing health care services for a patient which may be personally identifiable.

III. Procedure

All persons employed or volunteering at the SHC who have access to PHI must hold this information in strict confidence and adhere to the following expectations:

A. Training
   1. The University training in the Human Resourses Talent Management system- *Security Awareness Training* (upon hire)
   2. The SHC training in PowerDMS - *PHI/FERPA Privacy Training* (within the first 30 days and annually thereafter)

B. Staff will only access PHI in the SHC on a need to know basis. Any review of information by staff who are not directly involved in that patient's care or have not been directed to retrieve that information for the purpose of delivering, monitoring, or assessing health services will be considered a breach of confidentiality.

C. At no time shall staff or others associated with the SHC who have access to confidential information speak with media or others outside the SHC regarding SHC services without prior approval of the SHC Director as per SHC policy, *Student Health Center Representation*.

D. Requests for release of patient information will be processed per guidelines of SHC policy, *Release of Confidential Information Policy*.

IV. Attachments

None

V. References

1. AAAHC Standards 3.E.1-5, 6.B.1-5, and 6.D.1-2.

Electronic Health Records (EHR)

I. Policy

Electronic Health Records and all health care documentation should be treated confidentially in a manner complying with state and federal regulations (e.g., HIPAA). Student Health Center (SHC) staff will maintain primary responsibility for the care, distribution, protection, and utilization of the health records.

II. Procedure

A. Paper Records

1. Personal Health Information (PHI) recorded on paper should be filed and stored in a locked area that is protected from unauthorized individuals.
2. Paper records should be scanned into the patient's electronic medical record as soon as possible.
3. Once scanned into the EHR, the paper copy may be destroyed in a manner appropriate for confidential records as long as the paper copy does not have additional anticipated purpose.

B. Electronic Records

1. Electronic devices used to access the EHR should be locked each time the staff member steps away from his or her work area.
2. Patient records should **never** be left unattended or in view of unauthorized individuals.

III. Electronic Medical Record Content

A. Patient Demographics

1. Contact information
2. Name
3. Date of Birth
4. Gender/Gender preference
5. Insurance
6. Patient student Identification number
7. Billing Method
8. Communication Preference
9. Consent to treat/Financial policy
10. Consent Forms: as Necessary

B. Patient Summary

1. Allergies
2. Current Medication
3. Social History
4. Medical History
5. Family History

6. Surgery History

C. Intake

1. Date
2. Vital Basic
3. Female Exam Intake
4. Intake
5. Orthostatic Vitals
6. Peak Flow
7. Vision Screen Intake
8. Nurse Education/Counseling

D. SOAP Note

1. Subjective
2. Objective
3. Assessment
4. Plan

E. Progress Note

IV. Attachments

None

V. References

1. AAAHC Chapter 6 “Clinical Records and Health Information” , Standards A, B,C, E, D
2. Health Information Portability and Accountability Act
3. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
4. https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

.

SHC Disposal and Retention of Patient Health Information

I. Policy

The Student Health Center has the responsibility to ensure the privacy and security of its Patient Health Information. PHI and other confidential information shall be retained per SHSU and state regulations. Proper disposal methods for confidential information may include, but are not limited to shredding or burning the records and information so that it is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

II. Procedure

A. SHC Student Health Center PHI and other confidential information shall be retained in accordance with established SHSU, State and Federal regulations. Adult records will be kept for 7 years from the date of the last treatment and for minor patients records will be retained for 7 years after the date of the last treatment or until the patient reaches age 21, whichever date is later.

B. Electronic medical records for students who have graduated will be placed in an inactive folder in the Medicat system, 30 days after their graduation date.

C. The Student Health Center will contract with a certified document disposal company that specializes in the disposal of confidential documents and PHI.

D. Documents containing confidential and/or sensitive information (including PHI) to be shredded will be kept in a secure disposal canister in the building until pickup by the contracted document disposal company.

III. Reference

1. AAAHC Chapter 6 “Clinical Records and Health Information”, Standards 6.B and 6.D

2. Tex. Admin.Code 165.1(b) (2008)

3. Texas Medical Privacy Act, FERPA, HIPPA

4. https://www.dshs.texas.gov/records/medicalrec.shtm

GENERAL OFFICE POLICY & PROCEDURE

Ethics & Practice

Counseling Center staff and trainees adhere to the ethical principles of the American Psychological Association (APA) and the American Counselors Association (ACA). Additionally, all clinicians must adhere to the rules of practice outlined by the Psychologists' Licensing Act of the State of Texas and the Texas State Board of Examiners of Psychologists (TSBEP). Additional information can be found at:

American Psychological Association – www.apa.org/ethics/code/index.aspx
American Counselors Association – www.counseling.org/resources/codeofethics/TP/home/ct2.aspx
Psychologists' Licensing Act – www.tsbep.state.tx.us/act-and-rules-of-the-board
Texas State Board of Examiners of Psychologists – www.tsbep.state.tx.us

Dual/Multiple Relationships

Although not all dual/multiple relationships are inherently harmful or exploitative, such relationships should be avoided when possible in order to maintain appropriate boundaries. Given the size of SHSU and the surrounding community, however, the potential to encounter current clients in a variety of contexts is quite high. Clinicians should consult with peers when a possible dual/multiple relationship presents itself in order to process through relevant clinical and ethical considerations and determine an appropriate course of action. The outcome of such consultation should be documented in the appropriate location (e.g. a client's file, or the counselor's private notes).

Trainee/Student Clients

Due to the lack of clinical resources in the surrounding community, the Counseling Center represents the best option for services for many students; including students from academic departments that feed our training programs. Students who have completed a practicum at the Counseling Center are eligible to receive services, but these services cannot be provided by a previous clinical supervisor. Students who have previously received Counseling Center services are not eligible to complete a practicum at this center. Trainees do not provide services to students from their home program. Additionally, clinicians do not provide services to students who are enrolled in a class they are teaching.

Confidentiality

Confidential information may not be discussed with anyone outside of the Counseling Center, unless a signed release of information form has been obtained (Appendix B). The form must be signed and dated by the client, as well as by a witness other than the counselor named in the release. A signed release must be obtained before sharing information with a person or agency outside of the Center. This includes areas that are frequent sources of collaboration or referral, such as the Dean of Students Office, Department of Athletics, Services for Students with Disabilities, and Student Health Center (a separate form exists for these last two offices).

Please keep in mind that other departments on campus, and many off campus agencies, have their own standards for the sharing of information related to critical incidents. Typically, this means that information can be shared with minimal restriction and they may expect the same of us. In such instances it may be necessary to provide a friendly reminder that as licensed clinicians, psychologists are legally and ethically bound to a higher standard regarding privacy and that as a result we likely can't participate in the quid-pro-quo sharing of information.

When a parent or concerned other calls with information about a current client, they often expect an update or specific guidance about said client. Such individuals should be informed that without a signed release a client's attendance can't be confirmed and clinical information can't be shared. They, however, are free to share relevant information with us and the consulting psychologist can provide them with general guidance.

Given the Counseling Center's open floor-plan and limited sound-proofing, please me mindful of your surroundings when discussing confidential information. Ideally, any conversation involving clinical or identifiable information should take place behind closed doors.

Mandated Reporting

In the state of Texas, a client's confidential information can be shared in the following instances, due to mandatory reporting requirements:

a) If a client is determined to be in imminent danger of harming him/herself.
b) If a client discloses current abuse or neglect of children (ages 17 and under), the elderly (ages 65 and above), or disabled persons.
c) If a client discloses sexual misconduct by a therapist.
d) If a court issues a subpoena for records as part of a judicial proceeding.

For additional information, please refer to the following statutes:

Duty to Report Child Abuse and Neglect – Texas Family Code, Chapter 261, Subsection B

Duty to Report Abuse of Elderly or Disabled Person – Texas Human Resource Code, Chapter 48, Subsection B

Duty to Report Sexual Exploitation of a Patient by a Mental Health Services Provider – Texas Civil Practice and Remedy Code, Chapter 81, Section 81.006.

When it comes to mandated reporting please keep in mind that the state of Texas does not legally recognize a duty to warn identifiable third parties when threats of violence have been made against them by a therapy client. This may be at odds with training that clinicians at the Counseling Center have received in other jurisdictions, in addition to an individual's personal ethics, but it is an important element of practice here. In the rare instance that a clinician must decide whether to break confidentiality in order to protect an identifiable victim, consultation with the Director or Assistant Director must be obtained before any action is taken. All legal requests for client records from attorneys or the courts should be brought to the attention of the Director or Assistant Director immediately, and before any information is released.