

**Sam Houston State University**  
**A Member of The Texas State University System**

**Finance & Operations Information Resources Policy FO-IR-09**  
**Information Security Policy and Plan**

**I. Background**

Sam Houston State University has established this policy in an effort to satisfy two University goals. The first goal being to clearly define the University's Information Security Policy in order to provide a guide for SHSU personnel to assure ongoing compliance with federal, state and university information security policies. The second goal is to provide a detailed explanation for the SHSU community as to how the university will ensure the privacy and integrity of their personal information.

**II. Definitions**

- a. University Community --- Faculty, staff, students, retirees, alumni and other related individuals of SHSU
- b. Private Information / Personal Information --- Information deemed to be public record by federal or state law.
- c. Administrative Request --- Request for information by university administrators or the Information Security Plan Coordinator.
- d. Safeguards --- Policies and procedures responsible for ensuring the security and privacy of the SHSU information system and its data.
- e. University Information ---All data stored within the SHSU Information System. Information includes both paper and electronic records.
- f. University-designated Owner of the Information --- Computer Services-designated owner of a category of university information.

**III. Security Plan Coordinator**

The University has designated the Associate Vice President for Information Resources as the Information Security Plan Coordinator (hereinafter referred to as the Coordinator). The Coordinator will work closely with SHSU's Information Technology security staff, application development staff, and Internal Auditor's office. Additionally, all academic and administrative areas will be collaborators to gather information, coordinate training and awareness, and ensure compliance with this security policy. SHSU will consult with The Texas State University System General Counsel's office as well.

The Coordinator will assist University departments in identifying internal and external risks to the security, confidentiality, and integrity of information; evaluating the effectiveness of the current safeguards for controlling these risks; designing and implementing new safeguards, and ensuring compliance and regular assessment of risks. The Coordinator will be responsible for updating this plan as necessary to reflect changes in federal, state, or university policy or procedures related to information security. The Coordinator will maintain and ensure this plan is available to the university community. All correspondence regarding this policy should be directed to the Plan Coordinator at (936)294-1158 or [marka@shsu.edu](mailto:marka@shsu.edu). The University Internal Auditor's office may also be contacted in the event of an emergency at (936)294-1975.

**IV. Departmental Roles**

Each SHSU academic and administrative area must ensure compliance with this policy within their area of supervision. Additionally each area is responsible for developing specific complementary policies related to their own areas, if needed. Copies of departmental security policies must be provided to the Coordinator for filing with the University plan.

Departments are responsible for ensuring that prior to being provided access to SHSU information, faculty and staff read and acknowledges receipt of this policy. Departments are responsible for maintaining a permanent record of this acknowledgement and must be able to provide it upon administrative request. Departments should also be able to produce documentation of their internal training procedures upon administrative request.

**Sam Houston State University**  
**A Member of The Texas State University System**

**IV. SHSU Information Systems**

SHSU has developed an information access system based on the principle that users are only allowed access to information if previously authorized access by the owner of the information category. The existence of a single university information database further facilitates the university's ability to ensure security of the information according to this Information Security Plan. Each access interface to SHSU's information database will only display university information after the appropriate access information has been provided by the user. Existing SHSU Computer Services policies that prohibit multiple users from using a single system logon also help to maintain information security in accordance with this plan.

**V. Family Educational Rights and Privacy Act (FERPA) also referred to as the Buckley Amendment**

- a. SHSU abides by the rules set forth by FERPA
- b. Details are posted online. <http://www.shsu.edu/administrative/policies/pdf/ferpa.pdf>
- c. Information is also posted in the Schedule of Classes each semester. "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) E-mail Address, (7) Enrollment Status, FT/PT, (8) Degrees, Diplomas, and Certificates and Date of Award, (9) Honors and Awards, (10) Classification, (11) Extracurricular Activities, (12) Birth date and Place of Birth, (13) Names and Addresses of Parents/Legal Guardians, (14) 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 the above information is not to be released. A student may restrict the release of directory information by using the SamInfo Link on our home page [www.shsu.edu](http://www.shsu.edu) or submitting written notification to the Registrar's Office, Estill 331. Notification must be given prior to the twelfth class day of the fall and spring semesters and the fourth class day of each summer term. 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. In addition, a student's name will not be published in the Deans List, the Commencement Program, or the Honors List at Commencement, when the Buckley has been invoked. 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"."

**VI. Categories of Risk**

The University has identified the following primary risk categories and established the corresponding policies.

- a. Electronic Information
  - i. Categories include but are not limited to:
    1. Information displayed by a university information system application or user application where the data was originally acquired from the university information system
    2. Information stored on removable media (ie. Flash disk, CD, Zip....) if it originated from the University information system
  - ii. Policies include but are not limited to:
    1. Users must be currently logged in with their University-assigned computer account when accessing the University information system.
    2. Upon entry of a new category of information into the University information system, Computer Services will designate an owner for the information who is responsible for the authorization and revocation of user access to this information.
    3. Logon notices are displayed informing users of their responsibility to ensure information privacy.

**Sam Houston State University**  
**A Member of The Texas State University System**

4. Data storage devices that may contain private information must be erased prior to disposal.
  5. University information system data may not be reproduced electronically unless in direct relation to authorized university activities.
  6. Data storage devices that may contain private information may not be released to other individuals.
  7. Information may be released when in direct relation to authorized SHSU activities and contracts.
  8. Any loss of information must be immediately reported to the supervisor and the Information Security Plan Coordinator.
- b. Hard Copy Information
- i. Examples include but are not limited to:
    1. Information printed by a University information system application or user application where the data was originally acquired from the University information system.
    2. Information printed from removable media (ie. Floppy disk, CD, Zip....) if the information originated from the University information system.
    3. Handwritten Information that originated from the University information system.
  - ii. Policies include but are not limited to:
    1. Users must be currently logged in with their SHSU-assigned computer account when printing from the university information system.
    2. Printed information of a private nature must be shredded when no longer needed.
    3. Printed information of a private nature must not be released without approval of the owner of the information.
    4. Printed information must not be left viewable in a publicly accessible area.
    5. Information may be released when in direct relation to authorized University activities and contracts
    6. Any loss of information must be immediately reported to the supervisor and the Information Security Plan Coordinator
- c. Verbal Information
- i. Examples include but are not limited to:
    1. Spoken release of information originally obtained from the SHSU information system
  - ii. Policies include but are not limited to:
    1. Private information originating from the SHSU information system will not be provided verbally over the phone without additional identity verification.
    2. Information originating from the SHSU information system about an individual will only be released to that individual and only upon the individual presenting proper identification.
    3. Information may be released when in direct relation to authorized University activities and contracts.
- d. Application Development
- i. Examples include but are not limited to:
    1. Software developed to provide access to the SHSU information system
    2. Software developed to provide access to information that was originally obtained from the SHSU information system.
  - ii. Policies include but are not limited to:

**Sam Houston State University**  
**A Member of The Texas State University System**

1. Prior to deployment, all applications that access the University information system will be reviewed by Computer Services Quality Control to evaluate and address privacy issues.
2. Applications not approved by Computer Services Quality Control will not be installed for access by the university community or general public.
3. Applications will be made available to only those authorized to access the data within the application.

**e. Other**

- i. Any method of accessing or providing access to University Information must adhere to the above rules.

**VII. Training and Education**

The University will provide training during new employee orientation to familiarize employees with this Information Security Plan. During employee orientation employees will receive specific training on the importance of ensuring the confidentiality of information and will be informed of proper computer use, computer account security, document handling and verbal release of information. New employee training will also include education on relevant University policy, procedures and safeguards established to ensure the privacy of University community information. Additionally job-specific training will be provided by all academic and administrative areas throughout the University.

University community training and education will also include newsletters, promotions or other programs to increase awareness of the importance of maintaining the confidentiality and security of information.

The University has adopted comprehensive policies, standards and guidelines setting forth the procedures and recommendations for maintaining the integrity and the security of information kept within the University information system. For additional information on these please refer to the Sam Houston State University *Administrative Policies and Procedures*.  
<http://www.shsu.edu/administrative/policies/>

**VIII. How to Obtain and/or Correct Information**

- a. Students
  - i. Contact the SHSU Registrar's office
  - ii. [http://www.shsu.edu/~reg\\_www/](http://www.shsu.edu/~reg_www/)
- b. Faculty/Staff
  - i. Contact the SHSU Human Resources department
  - ii. [http://www.shsu.edu/~hrd\\_www/](http://www.shsu.edu/~hrd_www/)

**IX. Third Party Contracts**

If SHSU deems it necessary to contract with a service provider, and if in fulfillment of this contract, the service provider is provided access to SHSU information originating from the University information system, the contract will specify constraints to ensure the privacy and integrity of the University information. When choosing a service provider, an evaluation will be conducted to review the service provider's ability to safeguard customer information. Results of the evaluation must be provided to and approved by the Security Plan Coordinator and University Internal Auditor's office prior to contract approval. Vendors that are unable to achieve a satisfactory evaluation will not be selected. Upon selection of a service provider, the results of the evaluation will be filed with the approved final contract. Contracts with service providers will include the following provisions:

- a. An explicit acknowledgement that the contract allows the contract partner access to confidential information;
- b. A specific definition or description of the confidential information being provided;
- c. A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

**Sam Houston State University**  
**A Member of The Texas State University System**

- d. An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- e. A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract
- f. A provision allowing auditing of the contract partner's compliance with the contract safeguard requirements;
- g. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the University to terminate the contract without penalty;
- h. A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract; and
- i. A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

**X. Public Notification of Privacy**

The University will provide as part of the class registration process and employee hiring process, notification to the individual of this Information Security Plan. The University will maintain a permanent notice on the University web site in order to comply with the need for an annual notice. The notice must inform the individual of their right to choose to not have their information released publicly and how the individual may activate this right.

**XI. Risk Assessment**

The Security Plan Coordinator will coordinate an annual risk assessment to evaluate the overall effectiveness of the University's Information Security Plan and its ability to address changes that have occurred during the previous year. This assessment will require all academic and administrative areas throughout the University to assess their information access and information security procedures and policies. Departments will submit the results of the risk assessment to the Information Security Plan Coordinator along with any new local policies that have been developed to address problems. The results of the Risk Assessment will be summarized by the Information Security Plan Coordinator. Based upon the results of the assessment and administrative recommendations the Information Security Plan Coordinator will update this plan as necessary to ensure and maintain information security.

**XII. How to update this plan**

The SHSU Information Security Plan is administered by the Information Security Plan Coordinator as identified in section III. If you have questions about this plan or would like to request additions or changes please contact the Information Security Plan Coordinator.

**XIII. Where is this Plan Located**

This Information Security Plan is included as part of the University Administrative Policies and Procedures on the Sam Houston State University Web site.  
[http://www.shsu.edu/administrative/policies/pdf/sh\\_info\\_sec\\_plan.pdf](http://www.shsu.edu/administrative/policies/pdf/sh_info_sec_plan.pdf)

**Related Legislation and Policies**

- a. Financial Services Modernization Act (Gramm-Leach-Bliley)
  - i. Federal law that protects the privacy of information gathered from "banking relationships"
  - ii. 15 U.S.C. § 6801-6809
  - iii. <http://www4.law.cornell.edu/uscode/15/ch94sch1.html>
  - iv. [http://www.ftc.gov/privacy/privacyinitiatives/financial\\_rule.html](http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html)
  
- b. Family Educational Rights and Privacy Act (FERPA)
  - i. Federal law that protects the privacy of student education records

**Sam Houston State University**  
**A Member of The Texas State University System**

- ii. 20 U.S.C. § 1232g; 34 CFR Part 99
  - iii. <http://www4.law.cornell.edu/uscode/20/1232g.html>
  - iv. <http://www.ed.gov/offices/OII/fpco/ferpa/>
- c. Texas Open Records Act
- i. State Law that provides public access to government records
  - ii. <http://www.shsu.edu/~acc/www/policies/policy1.html#open>
  - iii. <http://www.capitol.state.tx.us/statutes/go/go0055200toc.html>
- d. PCI\_DSS: Payment Card Industry Data Security Standard
- i. A worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The PCI security standards are technical and operational requirements that were created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats.
  - ii. <https://www.pcisecuritystandards.org/>
- e. The Health Insurance Portability and Accountability Act (HIPAA)
- i. HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.
  - ii. <http://www.cms.hhs.gov/HIPAAgenInfo/>
- f. Texas Administrative Code (TAC 202)
- According to Texas law, all state agencies must meet or exceed the standards set forth in Chapter 202 of the Texas Administrative Code.
- i. [http://info.sos.state.tx.us/pls/pub/readtac\\$ext.ViewTAC?tac\\_view=4&ti=1&pt=10&ch=202](http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202)

Reviewed by: Mark C. Adams, Associate Vice President for Information Resources - 04/20/2009  
Next review: 04/20/2010