

New Employee Technology Orientation

Computer Services
Sam Houston State University
A Member of the Texas State University System

Information

SHSU Computer Access information for New Employees:

SAM ID #: Purpose: Unique campus ID number. Used in public areas rather than social security number.

Computer Login ID: Purpose: This will be the user ID used to logon to campus computer resources.

Computer Login password: You will set this when you activate your computer account.
Purpose: Used in combination with your "computer login ID" to authenticate your computer access.

PIN: Your personal ID number. A six digit number. The default is your birthday in MMDDYY format.

Purpose: Used as a password identifier for initial computer account setup and some SHSU systems access.

Note: Recommend you reset this to number that only you know.

Email Address: Purpose: The official email account for you at SHSU.

Email Alias: Purpose: This can be used as a user friendly email address that is tied to your official email. In other words, when you access your email you will see email sent to

Computer Account Activation:

- 1) Select the "SAMWEB" option in the orange box on the left side of the SHSU home page www.shsu.edu
- 2) Scroll down to "Alternate Login" and use your SAMID and PIN from above to login.
- 3) You will be prompted to confirm you identity and then begin the activation process.
- 4) You will need to enter a password.
 - a. The password must be a combination of letters, digits, and special characters. We recommend a password between six and nine characters. The maximum length to work on all SHSU computing systems is 14 characters.
 - b. Your password must include characters from three of the following categories: lower case letters, upper case letters, numbers, and special characters such as the underscore (_) and the exclamation point (!). Do NOT use | > < * ' " within your password.

PIN Change:

- 1) Select the "SAMWEB" option in the orange box on the left side of the SHSU home page www.shsu.edu
- 2) Login with your SHSU username and password
- 3) Select the "Student Records" option at the left of the screen.
- 4) Select the "PIN Change" option at the left of the screen.
- 5) Enter a six digit number that only you will know.

Email Access:

- 1) Select the "Exchange Mail" option in the orange box on the left side of the SHSU home page. www.shsu.edu



- 2) Login with your SHSU username and password.

Workstations and Nodes

Workstations are called "nodes" when attached to the SHSU network. The naming convention is used to give every computer on the SHSU network a unique name and identifier. These names are assigned by Computer Services when the machine is built or received from Dell. Our scheme is a three-part name with the building abbreviation, the floor number, and the computer number for that floor, all separated by a dash. For example, AB1-1-114 is a machine in the AB1 building, on the first floor. When calling the Helpdesk for support, you will be required to provide the node name of your computer so that they can better diagnose any problems. The node name is normally found on a white sticker on the top of the tower or case. It can also be found on the Start Menu, right-hand side as an icon of a computer with the label "*username on node number.*"

Microsoft Windows XP

SHSU uses Windows XP as the default operating system for the machines connected to the network. New machines received are installed with the XP operating system. You will have customized settings and programs that are available wherever you log in.

Windows Account and Password

Each employee and student at SHSU is given a username and a password in order to log into the network. This username and password also grants access to Sam Menu, SamWeb, e-mail and Blackboard. When you log onto any machine on campus running Windows XP (MACS are on a separate network) they are connected automatically to their specific network resources, along with the resources of the local machine. The network resources include the S:, R:, and T: network drives. To log into an XP machine, press Control + Alt + Delete, enter your Windows username and password and click OK. *Windows passwords ARE case-sensitive.* You can reset your password online if needed through SamWeb. *Passwords are only good for one year.* Reminders will be sent within 60 days of the password expiration.

Equipment

Laptops

To connect your laptop to the Internet read the instructions linked at the end of the paragraph. When purchasing a laptop, we suggest that you purchase it with the Windows XP operating system. In addition, there is no need for you to purchase Microsoft Office for the laptop, since we have a campus license agreement with Microsoft. If you have questions about laptop issues, you can visit our software guides at <http://www.shsu.edu/guides>

Computer Labs

Computer Services has 12 computer labs across campus, manned by more than 70 lab assistants. Three of these are labs for students to use as general use; [AB4](#), [CHSS](#), and the left side of [NGL](#). All Computer Services labs are equipped with computer workstations, DVD-RW drives, scanners, printers, USB ports for access with compatible flash/USB drives, and other peripheral items.

[Kayla Stephenson](#) is the full-time lab manager. She is in charge of the hours of operation, maintenance of the labs and equipment, [lab reservations](#), and lab assistant scheduling. A list of computer labs is available at http://www.shsu.edu/~ucs_www/lab/. The lab reservation information is posted at http://www.shsu.edu/~ucs_www/lab/reserve.html.



Faculty and Staff members may use the University labs for classes, presentations, testing, etc. Faculty may submit problems with the lab conditions such as lighting, temperature, cleanliness, speed of connection, etc. to the Lab Manager at labs@shsu.edu. Faculty may view a [current calendar of labs reserved](#) for instruction and should view prior to submitting reservations. [Reservations must be made online](#). Reservations are scheduled on a first-come, first-serve basis. Labs must be reserved well in advance, preferably 2 weeks prior to the date you need it.

Visitor accounts needed for faculty or guest visitors can be requested through the helpdesk at 294-1950 or at helpdesk@shsu.edu. You will need to provide the guest's name and purpose for the account as well as how long the account will be needed.

Services

Network Services

SHSU LAN and Domain

The SHSU network is a Local Area Network. This LAN connection allows communication between computers and other devices on our domain called SHSU. Each workstation connected to the SHSU domain, is allowed to access the same resources, including network drives and domain servers. This connection is made with high-speed fiber optic and Ethernet cabling within and in between buildings. The physical connections are available in offices AND classrooms. Each office is set up with at least one active connection. This active line along with a correctly configured computer allows users to reach other buildings and web resources, as well as the Internet.

S: Drive

The S: drive is the personal network-based storage location for files and folders. Each person is allotted personal disk space on this network drive. As a faculty or staff member you may have a physical computer assigned to you. If you choose to store your documents on the local C: drive, you will want to make sure you make backups of these files on a regular basis. This is only suggested when you are the only user of that computer. If you roam from computer to computer, then you will want to store your documents on the S: drive for convenience and security. **REMINDER:** This storage location is a network-drive, so documents stored on the S: drive are not being saved to your local machine, but on a server. Your S: drive is only accessible by you, so it is also a more secure place to save sensitive documents.

T: or Common Drive

The T: drive is a location for faculty and staff to store documents that need to be shared with other network users. Many administrative and academic departments use this drive to store documents that only their department should access. The folders on the T: drive are named with abbreviations for that department, such as MKT for Marketing. Be aware that these folders are shared therefore they have limited security. In addition, you are not allowed to add new folders to the T: drive unless given special permission. If you need a folder on the T: drive, send email to the Helpdesk at helpdesk@shsu.edu to make the request. The folder will be set up with the requested permissions. The T: drive is for administrative use only and is checked daily for unauthorized files, such as MP3s. The policy for the T: drive and MP3s is found at <http://www.shsu.edu/~ucs/www/policies/mp3.html>

U: or UNX1 Home Directory

The U: drive is the storage location of personal Web pages. You are not connected to this drive when you log on by default. However, you can "map" or connect to this drive in order to be able



to “drag and drop” your Web page files to the server directly instead of having to telnet or FTP to move them over. Access to the U: drive requires the same username and password used for Windows. You can connect to your UNX1 home directory from an on-campus PC by going to Start → Programs → SHSU Utilities and selecting “Connect U: Drive to UNX1 Home Directory.” You will then be prompted to enter your password. After connecting to the U: drive, you will then be able to “drag and drop” items by finding the U: drive in Windows Explorer. You can reset your password online at <https://ww2.shsu.edu/acct01wp/index.php> .

E-Mail Account

Each employee on campus is provided with an e-mail account. The e-mail address for each person is their *username@shsu.edu* . The username and password combination to check your email is the same as the “Windows” username and password. E-mail can be checked either by using an e-mail application like Microsoft Outlook, or by using a browser such as Mozilla Firefox or Internet Explorer to access the SHSU web site and clicking Exchange Mail an online e-mail service provided by SHSU. Sam Houston e-mail can be checked either on-campus or off-campus. If you need help setting up an e-mail program to work with Sam Houston e-mail then call the helpdesk at 41950.



Roaming Profile

On SHSU computer network, you will have a desktop environment called your *roaming profile*. This profile consists of all the settings, the programs we installed for you, your desktop icons, as well as any programs that you have installed or used through the Start menu. The roaming profile is available by logging onto any of the networked Windows XP machines on campus. They are called roaming profiles because your settings, mail, bookmarks, etc, “go with you” wherever you go on campus. This service is not available off campus thru dial-in connection; however you may remote access your profile from home using remote.shsu.edu. If you are having problems with your machine or network connection and you get a question about logging on with a locally stored profile, please choose the download option. The locally stored profile is not consistent with what is on the network. Another question may also appear, asking if you want to use your locally stored profile. Answer NO to this question.

REMINDER: You will want to backup your profile regularly, by going to Start → Programs → SHSU Utilities → Backup and choose “Backup Profile.”

Quotas

The S: and U: drives and e-mail accounts are allotted a certain amount of storage space (a quota). Quotas are as following for Staff and Faculty:

S: Drive	1000 MB
Webpage	20 MB
Exchange	150 MB
Profile	35 MB

A profile management utility is available via Start Menu > Programs > SHSU Utilities > SHSU Profile Management Utilities to assist in managing profile materials.

Printing

You may have a networked departmental printer or a personal printer assigned for your use. From the Nell administrative system, you will print straight to PDF and it will be accessible from the SamWeb system. For more information, refer to our Technology Tutorial on [Adding Printers](#).



Wireless Connections

Computer Services provides wireless services throughout campus. Instructions on how to set up a wireless connection on your computer can be found in our Technology Tutorials:

<http://www.shsu.edu/guides>

Remote.shsu.edu

You are able to access your SHSU profile (including access to S:, T: and U: drives) from off-campus via a Remote Desktop Connection from an off-campus Windows computer. Instructions can be found in the Technology Tutorials located at <http://www.shsu.edu/guides>

Training and Support Services

SHSU Technology Tutorials

Technology tutorials are available online for many of the applications and services offered through Computer Services and SHSU. You can find this information by clicking the SHSU Help icon on the on-campus PC desktop or by visiting <http://www.shsu.edu/guides/>.

Computer Services Training

The monthly Computer Services training schedule is online at <http://www.shsu.edu/administrative/training/>. If you have requests for specific departmental training, please send e-mail to helpdesk@shsu.edu. Many have expressed interest in taking various Faculty/Staff training sessions but have found it difficult to attend at the scheduled times.

Helpdesk

The Helpdesk provides telephone support and assistance for most issues, including hardware, software, networking, profiles, accounts, printing, and dial-in connections. The Helpdesk is available by phone 24 hours a day by calling x4-1950 on campus, 294-1950 from off campus, (936)294-1950 for long distance or 1-866-BEARKAT toll free. For in-person help from the Helpdesk staff, the Helpdesk ([located in room 208 in Academic Building 1](#)) is open Monday – Friday, 8am to 5pm.

The Helpdesk is also responsible for nightly, weekly, and monthly backups of servers. Retrieval of lost data from backups is evaluated on a case-by-case basis. This is due to the length of time it takes to find and retrieve data from sequential backup tapes. If you have questions about recovering data from backups, please refer to the

Request for Restoral of Files for SHSU Faculty/Staff at

http://www.shsu.edu/~ucs_www/policies

Network Technicians

Computer Services provides in-house technical telephone, hardware, and software support through its team of network technicians. These technicians are responsible for maintaining and upgrading the physical lines and connections, workstations, and telephone systems.

Work Order System



The Computer Services Work Order system allows faculty/staff to place work orders with Computer Services through a web-based interface. Faculty/staff members can submit a Work Order for repair on their university computer, network/telephone, purchase requests for computer equipment, helpdesk support, submit website changes/corrections, and more. To access the Work Order System, visit <http://ww2.shsu.edu/word01wp/> (login required).

Sam Houston State University Home Page

The Sam Houston State University home page can be found at <http://www.shsu.edu> . The home page acts as a portal to all the major departments and functions of campus. The University Fast Links provide quick access to departments and functions most used by visitors to the page. There is access to the Internet, including search pages. The Intranet contains administrative materials for faculty and staff. In addition, various searches of Sam's materials and information can be made at the SHSU Search page located at <http://www.shsu.edu/search> or by using the search box on the homepage.

Each department is invited to have a web page, to facilitate easier access by all users to resources. E-Mail webdev@shsu.edu for help in matters concerning department web pages (or go to <http://webdev.shsu.edu/accessibility> for more information). To activate an account for web use, submit the Computer Account Request Form online at http://www.shsu.edu/~ucs_www/forms/computeracct.pdf.

SamWeb

SamWeb provides secure web-based access to programs for students and faculty/staff. Log in to <http://ww2.shsu.edu> to access these programs.

Blackboard

Blackboard can be used to enhance your lecture class with supporting information from the web, or it can be used for creating a standalone web-based class. Technology Support Services has a Blackboard FAQ page to answer most of your Blackboard question. You can access Blackboard by following the Fast Link from the SHSU web page or going directly to <http://blackboard.shsu.edu>. Training is also available on the Blackboard system, just email your request to blackboard@shsu.edu .



Administrative Services



Academic and Administrative Software

Computer Services works with many departments on campus to provide software for both administrative and academic purposes. These applications are available on networked XP machines. This software is configured for installation into your account (and S: drive) only. The programs available are located at Start menu → Programs → SHSU Programs. These programs are available, no matter where you log in on campus. If they are not on the SHSU Programs menu, they must be installed by contacting the Help Desk or Technology Support Services. The SHSU Program software is supported by the Helpdesk, and is licensed for network-wide campus use only.

NELL Administrative System

The SHSU administrative system is an Open VMS system called NELL and is the integral resource for admin departments. NELL is administered by Computer Services, but all the various departments on campus maintain its data. This system covers most information needs of both academic and administrative departments. Programs in the NELL system control the data exchange and sharing between departments, such as student information, grades, financial aid information, payroll, and many other specific tasks. This system required an account be created specifically based on your administrative functions. Your NELL password must be changed every ninety days. To change your password, launch NELL and type "set password" at the \$ prompt.

Each user has a default group of programs assigned to them and a personal menu to customize those frequently used programs. Users can request access to other programs depending upon job duties. You will be able to print out NELL reports to a networked printer. If you have any questions on NELL, you can call the **Helpdesk** at x4-1950. The Helpdesk is not able to issue passwords over the phone for security reasons. You must come to the Helpdesk in person (Academic Building 1, room 208), with your SHSU ID, to have the password changed.

SamMenu (GUI)

The GUI Menu programs are available by double clicking the SamMenu icon on the PC desktop and entering your Windows username and password. The SamMenu can also be installed and accessed off-campus using the instructions on <http://www.shsu.edu/faculty/menu.html>



General Information:

To request access, simply click on the program name listed under *Inaccessible Programs*. If you know the name of the program, select *Search for Program* under the *Help* option at the top of the screen. Enter the program name (or partial name) in the box provided. Expand the list of *Inaccessible Programs* by clicking it; click on the program name you wish to request. An e-mail will be sent to the owner of the program indicating that you have requested access.

Requesting Access for Student Workers:

To request access for a student worker, use *RQST01MG* under *Computer Services* on the Sam Menu. Enter the program name in the space provided and the username(s) of the student for whom you are requesting access. Using this program will allow program owners to track the origin of the request when reviewing their program lists and user access.

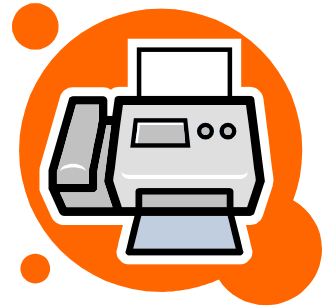
Program Owners:

For program owners, granting access from the Sam Menu is a similarly simple process. Upon

login to the Sam Menu, you will be notified of any pending requests that you may have. You may process those requests when you login to the menu by following the prompts as they appear or a later time by selecting "Manage User Access" under the Help option at the top of the screen.

NELL Web Printing

Printing from the web instead of from NELL directly provides users more printing options. Any user can enter in WEB as the destination and LP11 as the printer type and the NELL print job will go to a holding place in our web server. From <http://ww2.shsu.edu/> you will be able to login using your Windows username and password and see the jobs waiting to print. Select the job you want to print and it will open in Adobe Acrobat. Opening these documents in Adobe Acrobat allows the user to print all or portions of the document or even double-sided. This feature is available for most programs in NELL.



If you need assistance...

With Training, Tutorials or Web Development:

Thomas Sosebee..... x43476
Jurden Bruce x44495

With Computer Labs, Lab Equipment or Lab Assistants:

Lab Lead Worker Office..... x43463
Kayla Stephenson (Lab Manager)..... x43062

Other:

Helpdesk x41950
Switchboard 0

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. 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 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/
- b. Faculty/Staff
 - i. Contact the SHSU Human Resources department
 - ii. 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

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

- 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](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