Sam Houston State University

A Member of The Texas State University System
Division of Information Technology

INTEROFFICE MEMO

DATE: 01/04/2012

TO: MARK ADAMS
ASSOC VP FOR INFORMATION TECHNOLOGY

FROM: KAY KAY DAVIS
ASSISTANT VP FOR INFORMATION TECHNOLOGY

RE: POLICY FOR REVIEW

The attached three polices are submitted for cabinet review in order to comply with Texas Administrative Code guidelines and the current TSUS IT auditor policy review. These are three new policies to be added to the Division of Information Technology section of the official SHSU Policy page.

1. **IT-XXX Media Sanitization Policy** – This policy defines the requirements for removal of confidential information as outlined in TAC 202.

2. **IT-XXX Non-Disclosure Agreement Policy** – This policy defines the need and requirement for Non-Disclosure Agreements when accessing confidential information as outlined in TAC 202.

3. **IT-XXX Risk Assessment Policy** – This policy defines the requirements for IT risk assessments as outlined in TAC 202.

Sam Houston State University
Information Technology Services (IT@Sam)

Media Sanitization Policy: IT-XX

PURPOSE:

It is the policy of Sam Houston State University (SHSU) that all data must be removed from devices and equipment that are capable of data storage, transmission or receipt prior to equipment disposal.

IT@Sam Technical support staff will properly sanitize, as necessary, all information technology resources prior to transfer, sale or disposal. It is imperative that all devices capable of storing SHSU information be sanitized in a way that will make data recovery impossible.

This document establishes specific requirements for information technology media sanitization 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 Media Sanitization Policy applies to all SHSU owned or leased information technology.

POLICY STATEMENT:

Prior to the sale, transfer or disposal of information technology resources, IT@Sam technical support staff will take the appropriate steps, per the IT@Sam Property Office Media Sanitization Procedures, to ensure all data is removed from any associated storage device.

1. Information technology resources shall be sanitized utilizing a method that will ensure data recovery is impossible, such as degaussing, shredding, or destroying the media utilizing a destruction method that will be able to withstand a laboratory attack (e.g., disintegration, pulverization, melting or incineration).

2. If the device is a cell phone or PDA, remove subscriber identity module (SIM) and additional memory cards and destroy per sanitization requirements. Sanitize the unit utilizing a method that will ensure data recovery is impossible.

3. Document the removal and completion of the process with the following information:

    a. Date;
    b. Description of the item(s) and serial number(s);

c. Inventory number(s);
d. The process and sanitization tools used to remove the data, or process and method used to for destruction of the media; and
e. The name and address of the organization to which the equipment was transferred, if applicable.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Sam Houston State University

Information Technology Services (IT@Sam)

Non-Disclosure Agreement Policy: IT-XX

PURPOSE:

Nondisclosure agreements are contracts intended to protect information considered to be sensitive or confidential. Information technology resources shall be used only for intended purposes as defined by Sam Houston State University (SHSU) and in compliance with applicable laws.

All individuals are accountable for their actions relating to information technology resources and shall formally acknowledge that they will comply with the Sam Houston State University security policies and procedures or they shall not be granted access to confidential information. All employees requesting access to confidential information will complete a non-disclosure agreement for information technology resources on an annual basis.

This document establishes specific requirements for Non-Disclosure Agreements at Sam Houston State University. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202); Texas Administrative Code, Title 1, Part 10, Chapter 203, Subchapter B (TAC 203); and TSUS Rules and Regulations; Chapter III, Paragraph 19)

SCOPE:

The Non-Disclosure Agreement Policy applies to all users who utilize SHSU's information technology resources (including, but not limited to, Faculty, staff, student workers, temporary employees, vendors, consultants, employees of independent contractors, and personnel from other universities.)

POLICY STATEMENT:

All users must sign a SHSU Non-Disclosure Agreement (NDA) acknowledging they have read and understand SHSU requirements regarding computer security policies and procedures prior to being granted access to confidential information. This signed non-disclosure agreement becomes permanent record and will be renewed annually.

Electronic signatures are an acceptable means of acknowledgement of SHSU's Non-Disclosure Agreement.

Data Owners will facilitate and manage the respective annual NDA acknowledgment for their data.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Sam Houston State University

Information Technology Services (IT@Sam)

IT Risk Assessment Policy: IT-XX

PURPOSE:

IT Risk assessments are designed to assess the security posture of a system or application with the purpose of management's awareness of the major security risks in the SHSU infrastructure and to propose recommendations for mitigation of these risks.

The principal goal of a IT risk management process is to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out only by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

IT Risk assessments may be conducted on a regular basis throughout the System Development Life Cycle and/or on an ad-hoc basis in response to specific events such as when major modifications are made to the system's environment or in response to a security incident or audit.

This document establishes specific requirements for Information Technology risk assessments 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 Risk Assessment Policy applies to all stakeholders involved in preserving the confidentiality, integrity and availability of SHSU information technology resources including software, data, and hardware. This encompasses, but is not limited to SHSU Management, System and Data Owners, users, and Information Security Personnel.

POLICY STATEMENT:

Appropriate security levels and data control requirements must be determined for all information technology resources based on SHSU confidentiality, integrity and availability requirements for the information, as well as its criticality to SHSU's business mission and legal requirements.

Risk assessments will be performed according to the SHSU IT Risk Assessment Procedures to identify threats and vulnerabilities, document weaknesses identified, analyze findings, evaluate strategies, remediate/mitigate risks, and document acceptable risks.

The frequency of recurring assessments will be determined by the system or data owner's ranking of the information technology resources or when system changes, incidents, or audit findings require that another risk assessment be performed.

The following identifies the key roles of the personnel who are responsible for the protection of SHSU information technology resources and participate in the risk management/assessment process.

The **DATA OWNER** or designated representative(s) are responsible for and authorized to:

1. Determine and document the asset's value, inherent risk and rank (high, medium or low) according to TAC 202 criteria and outlined in the SHSU Risk Assessment Procedures.
2. Specify data control requirements and convey them to users and custodians;
3. Specify appropriate controls, based on risk assessment, to protect the Agency's information technology resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information technology resources outsourced by the Agency;
4. Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data;
5. Approve user access(access list) to an information technology resource asset and ensure compliance with applicable controls;
6. Review access lists based on documented Agency security risk management decisions.
7. Assign custody of information technology resource assets and provide appropriate authority to implement security controls and procedures; and

DATA CUSTODIANS of information technology resources, including third party entities providing outsourced information technology resource services to state institutions of higher education shall:

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

USERS of information technology resources shall:

1. Users shall use the resources only for defined purposes and comply with established controls;
2. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of that data; and
3. If any user is aware of a possible weakness in the protection of data, he or she must report their concerns to the Information Security Group.

The **INFORMATION SECURITY OFFICER** is the administrator of the SHSU information security program and shall:

1. Develop and recommend policies and establish procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information technology resource assets against unauthorized or accidental modification, destruction, or disclosure.
2. 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).
3. Is responsible for monitoring the effectiveness of defined controls for mission critical information.
4. 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 resource security controls.
5. 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.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Sam Houston State University

A Member of The Texas State University System
Division of Information Technology

INTEROFFICE MEMO

DATE: **JANUARY 20, 2012**

TO: **MARK C. ADAMS**
ASSOCIATE VICE PRESIDENT FOR INFORMATION TECHNOLOGY,
INFORMATION TECHNOLOGY SERVICES

FROM: **KAY KAY DAVIS**
ASSISTANT VICE PRESIDENT FOR INFROMATION TECHNOLOGY
INFORMATION TECHNOLOGY SERVICES

RE: **POLICIES FOR REVIEW**

The attached fourteen polices are submitted for cabinet review in order to comply with Texas Administrative Code guidelines and the current TSUS IT auditor policy review. These are three new policies to be added to the Division of Information Technology section of the official SHSU Policy page.

1. **IT-03 Acceptable Use Policy** – This policy defines the acceptable use of information resources technology as outlined in TAC 202.
2. **IT-XXX IT Administrator/Special Access** – This policy defines the requirements for users that are granted elevated account privileges as outlined in TAC 202.
3. **IT-XXX Application Security Policy –** This policy defines the requirements of applications that contain confidential or sensitive information as outlined in TAC 202.
4. **IT-XXX Authorized Software Policy –** This policy defines the requirements of software that can be installed or accessed on University-owned information technology resources as outlined in TAC 202.
5. **IT-XXX Electronic Communication Policy –** This policy defines the acceptable practices electronic communication as outlined in TAC 202.
6. **IT-XXX Firewall Policy -** This policy defines the requirements of securing communications between different segments of the University network where different levels of security is warranted as outline in TAC 202.
7. **IT-XXX Identification/Authentication Policy -** This policy defines the requirement of authenticating users to ensure the security and integrity of SHSU data as outlined in TAC 202.
8. **IT-XXX Intrusion Detection/Prevention and Security Monitoring Policy –** This policy defines the requirement of monitoring, logging and retention of traffic that transverse SHSU networks to confirm that security practices and controls are in place to secure all SHSU information technology resources as outlined in TAC 202.

9. **IT-XXX Malicious Code Policy -** This policy defines the requirement of resistance to, detection of , and recovery from the effects of malicious code as outlined in TAC 202.
10. **IT-XXX IT Physical Access Policy -** This policy defines the requirement of access to IT@Sam data center, network closets, and protected IT facilities to minimize unauthorized access to these locations as outlined in TAC 202.
11. **IT-XXX Portable Computing Policy -** This policy defines the requirement for safeguarding electronic devices that can contain protected data as outlined in TAC 202
12. **IT-XXX Privacy Policy –** This policy defines the expectation of privacy to SHSU information technology users as outlined in TAC 202.
13. **IT-XXX System Development & Acquisition Policy –** This policy defines the planning, management and business processes associated with the development or acquisition of system that contain protected data as outlined in TAC 202.
14. **IT-XXX Third Party Access Policy –** This policy defines the standards for connecting to SHSU information technology resources to minimize the potential exposure to SHSU form damages which may result from unauthorized use of SHSU information technology resources as outlined in TAC 202.

Huntsville, TX 77341-2449 * 936.294.1950 * Fax 936.294.1231 * helpdesk@shsu.edu * www.shsu.edu/~ucs_www/

Sam Houston State University
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 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;
   e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws; or,
   f. Restricting or denying access to the system by legitimate users.
2. Users must not allow 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 material which SHSU may deem to be offensive, indecent or obscene (other than in the course of academic research or authorized administrative duties where this aspect of the

research or work has the explicit approval of the SHSU official processes for dealing with academic ethical issues).

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, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of SHSU Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XXX, 2012
Next Review: November 1, 2013

Sam Houston State University
Information Technology Services (IT@Sam)

IT Administrator/Special Access: IT-XX

PURPOSE:

The purpose of this policy is to provide a set of measures that will mitigate information security risks associated with IT Administrators/Special Access.

IT Administrators/Special Access is defined as users that have elevated account privileges. Therefore, these privileges must be restricted and granted only to those with an academic or business justification. Administrator accounts and other special-access accounts may have extended and overarching privileges. Thus, the granting, controlling and monitoring of these accounts is extremely important to the overall SHSU information security program. The extent of access privileges granted or used should not exceed that which is necessary.

SCOPE:

The SHSU IT Administrator/Special Access Policy applies equally to all individuals who have, or may require, special access privilege to any SHSU information technology resources.

POLICY STATEMENT:

Appropriate security levels and requirements must be determined for all special access accounts that utilize SHSU information technology resources. In order to safeguard information technology resources, the following controls are required:

1) All users of Administrative/Special Access accounts must have account-management instructions, documentation, training, and authorization.
2) All users must sign the SHSU Non-Disclosure Agreement before access is given to an account.
3) Each individual who uses special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
4) Each account used for special access must comply with the "Passwords" guidelines stipulated in the SHSU User Accounts Password Policy (IT-02).
5) The password for a shared special access account must change when an individual with the password leaves the department or SHSU, or upon a change in the vendor personnel assigned to the SHSU contract. The account must also be re-evaluated as to whether it should remain a shared account or not. (Shared accounts must be kept to an absolute minimum.)
6) In the case where a system has only one administrator, a password escrow procedure must be in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

7) When special access accounts are needed for audit, software development, software installation or other defined need. Special access must be:

   a) Authorized by the system owner, Information Resource Manager, or Information Security Officer. (E.g., IT@Sam Client Services is the system owner for all SHSU desktops, laptops, and tablets.)
   b) Created with a specific expiration date or annual review date.
   c) Must be removed when work is complete.

8) All privileged commands issued in association with special access must be traceable to specific individuals via the use of comprehensive logs.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Application Security Policy: IT-XX

PURPOSE:

The purpose of the Application Security Policy is to avoid inadvertent release of confidential or sensitive information, minimize risks to users and the University, and ensure the availability of critical applications.

SHSU focuses its efforts on security applications that hold or utilize data sets containing student information/records, personally identifiable information such as social security numbers or credit card numbers, and other categories of data that are protected by federal or state laws or regulations. Ultimately, to ensure application availability and reliability, all applications must be secured regardless of the type of information they utilize.

SCOPE:

The Application Security Policy applies to applications developed by university staff as well as to those acquired from outside providers. All applications are subject to this policy regardless of whether the application is hosted on university equipment or elsewhere.

POLICY STATEMENT:

To keep risk to an acceptable level, SHSU shall ensure that the proper security controls will be implemented for each application. Data owners, custodians, system administrators, and application developers are expected to use their professional judgment in managing risks to the information, systems and applications they use and support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

1. IT@Sam, individual departments, and contractors shall implement application security standards to have effective controls over systems they directly manage.

    a. If IT@Sam manages an environment or application, IT@Sam shall be responsible for implementing the application security controls.
    b. If a department manages an environment or application, that department shall be responsible for implementing the application security controls.
    c. If an outsourced contractor manages an SHSU environment or application for an individual department, the department must ensure that the contractor implements the application security controls.

2. Applications installed or being changed should follow the standardized application lifecycle established by the IT@Sam Project Lifecycle.

3. Each individual user (whether a developer, administrator, or user) should have a unique set of credentials for accessing a computer application.

4. Authenticated users should have access to a computer application and should only be allowed to access the information they require (principle of least privilege).

5. Establishing and changing access for a user or group should be approved by the application's data owner.

6. Developers should follow best practices for creating secure applications with the intention being to minimize the impact of attacks.

7. Developers should not develop or test an application against production data sources.

8. Logs for the server, application and web services should be collected and maintained in a viewable format for a period of time specified by applicable state regulations.

9. Maintain a full inventory of all applications, to include authentication and authorization systems, the data classification and level of criticality for each application.

10. Document clear rules and processes for reviewing, removing, and granting authorizations.

11. Review and remove all authorizations for individuals who have left the university, transferred to another department, or assumed new job duties on at least a semi-annual basis.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Authorized Software Policy: IT-XX

PURPOSE:

Authorized software is any software that is acceptable for use on SHSU information technology resources. The purpose of the Authorized Software Policy is to provide a set of measures that will mitigate information security risks associated with authorized software.

SHSU has negotiated special pricing and licensing for a variety of software available to all students, faculty and staff. Other software is readily available in the open market place that has some kind of licensing agreement under which the user is subject. Some software is considered to pose a security threat to SHSU and its use may be restricted.

Users entrusted with SHSU information technology resources are responsible for maintaining licensing information for any software the user installs, and if requested by the University, must provide SHSU with licensing information. This includes, but is not limited to, smart phones, ipads, tablets, laptops, etc.

Non-compliance with copyright laws regarding software is subject to civil and criminal penalties imposed by federal and state laws. These penalties are applicable to the University and/or an individual.

SCOPE:

The Authorized Software Policy applies to all users of SHSU information technology resources.

POLICY STATEMENT:

All software installed or used on University-owned information technology resources must be appropriately licensed.

IT@Sam Client Support Services shall maintain sufficient documentation to validate that the software is appropriately licensed. Persons installing or authorizing the installation of software should be familiar with the terms of the agreement.

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:

1. Do not illegally distribute or share software with anyone.
2. All software must be license compliant, including personally purchased software.
3. All software licenses must be readily available.

4. Report any suspected or known misuse of software to IT@Sam Client Support Services.

The following general categories of software are specifically prohibited on all SHSU Information Technology Resources unless specifically authorized by the Information Security Officer:

1. Software used to compromise the security or integrity of computer networks and security controls such as hacking tools, password descramblers, network sniffers, and port scanners.
2. Software that proxies the authority of one user for another, for the purpose of gaining access to systems, applications, or data illegally.
3. Software which instructs or enables the user to bypass normal security controls.
4. Software which instructs or enables the user to participate in any activity considered a threat to local, state or national security, including the assistance or transfer of information leading to terrorist activity or construction or possession of illegal weapons.
5. Any other software specifically prohibited by the Information Security Officer.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Electronic Communication Policy: IT-XX

PURPOSE:

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.

SHSU electronic communication services support the educational and administrative activities of the University and serve as a means of official communication by and between users and SHSU. The purpose of this policy is to ensure that these critical services remain available and reliable, and are used for purposes appropriate to the University's mission.

This policy is established to establish prudent and acceptable practices regarding the use of electronic communication; and to educate individuals using electronic communication with respect to their responsibilities associated with such use.

SCOPE:

This policy applies to all members of the SHSU community who are entitled to electronic communications for the purpose of sending, receiving, or storing of electronic messages.

POLICY STATEMENT:

Under the provisions of the Information Resources Management Act (Texas Government Code, Title 10, Subtitle B, chapter 2054), information technology resources are strategic assets of the State of Texas that must be managed as valuable state resources.

SHSU provides electronic communication services to faculty, staff and students, and to other affiliated classes of individuals, including alumni and official visitors. Use of SHSU electronic communication services must be consistent with SHSU's educational goals and comply with local, state and federal laws and university policies.

Communications via SHSU electronic systems are the property of SHSU, and management maintains the right to access when necessary. All user activity on SHSU information technology resource assets is subject to logging, review and open records.

All electronic communication activities must comply with the SHSU Acceptable Use Policy (IT-03).

The following activities are prohibited as specified by Texas Department of Information Resources in response to TAC §202 requirements:

- Sending electronic communication that is intimidating or harassing.
- Using electronic communication to transmit or receive material that may be offensive, indecent, or obscene.
- Using electronic communication for conducting personal business.
- Using electronic communication for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending electronic communication, except when authorized to send messages for another when serving in an administrative support role.
- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct agency business.
- Sending messages with excessively large attachments.
- Sending or forwarding electronic communication that is likely to contain computer viruses.
- All sensitive SHSU material or email containing sensitive data transmitted over external network must be secured during transmission.
- Electronic communication users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of SHSU or any unit of SHSU unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing SHSU. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Firewall Policy: IT-XX

PURPOSE:

SHSU operates external firewalls or gateways between the Internet and the SHSU network to establish a secure environment for the university's information technology resources. Internal firewalls are in place to establish secure communications between different segments of the University's network where different levels of security are warranted.

SHSU's firewalls are key components of the university's network security architecture. The Firewall Policy governs how the firewalls will filter traffic to mitigate the risks and losses associated with security threats to SHSU's information technology resources. This policy will attempt to balance risks incurred against the need for access.

The purpose of this policy is to protect SHSU's information technology resources from hacking and virus attacks by restricting access to information technology resources on the University campus. It is designed to minimize the potential exposure of SHSU to the loss of sensitive confidential data, intellectual property, and damage to public image which may follow from unauthorized use of SHSU's information technology resources.

SCOPE:

The Firewall Policy applies to all firewall devices owned and/or operated by SHSU.

POLICY STATEMENT:

Perimeter Firewalls:

The perimeter firewall permits the following outbound and inbound Internet traffic:

- *Outbound* - All Internet traffic to hosts and services outside SHSU's networks except those specifically identified and blocked as malicious sites.
- *Inbound* - Allow Internet traffic that supports the mission of the institution and is in accordance with defined system, application and service procedures.
- *Outbound/Inbound* – All internet traffic detected as malicious by the university's intrusion prevention system (IPS) and/or all traffic violating SHSU firewall policies is dropped.

Reason for filtering ports:

- Protecting SHSU Internet Users - Certain ports are filtered to protect SHSU information technology resources. The perimeter firewall protects against certain common worms and from dangerous services on SHSU information technology resources that could allow intruders access.

- Protecting our outbound bandwidth - If SHSU Internet users overuse their outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other SHSU systems.
- Protecting the rest of the Internet - Some filters prevent users from both knowingly or unknowingly attacking other computers on the Internet. In addition to being in SHSU's interests for protecting our bandwidth, it is the institutions' responsibility to prevent abuse of its network.

Roles and Responsibilities:

The Information Security Office is responsible for implementing, configuring and maintaining SHSU's firewalls and for activities relating to this policy.

1) At a minimum, firewalls must be annually tested and reviewed.
2) When there are major changes to the network requirements, firewall security policies will be reviewed and may warrant changes.
3) Firewalls must have alert capabilities and supporting procedures.
4) Auditing must be active to permit analysis of firewall activity.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Identification/Authentication Policy: IT-XX

PURPOSE:

The purpose of the Identification/Authentication Policy is to ensure the security and integrity of SHSU data and information technology resources by ensuring controls for securing user identification and authentication credentials. SHSU utilizes the three basic authentication methods: something you know (i.e., a password), something you have (i.e., smart card or ID), and something you are (i.e., fingerprint or other biometrics).

To ensure the security and integrity of SHSU data, identified users will securely authenticate to SHSU information technology resources and access only resources to which they have been authorized to access.

If user identities are not properly authenticated, SHSU has no assurance that access to information technology resources are properly controlled. This policy will mitigate the risk of unauthorized access of information, as well as establish user accountability and rules for access.

SCOPE:

The Identification/Authentication Policy applies to all individuals granted access to SHSU information technology resources.

POLICY STATEMENT:

SHSU shall require that systems are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication (any or all of the basic authentication methods), and implementing access controls on SHSU information technology resources. Access control is provided at the firewall, network, operating system, and application levels.

SHSU managers/supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties, as well as notifying Data Owners and IT@Sam of the termination of access to information technology resources.

Prior to being granted access to SHSU information technology resources, the needs of the employee, student worker, contractor, vendor, guest, or volunteer shall be given ample consideration and authorization granted to allow access to SHSU information technology resources. Access should be granted according to the principle of least privilege as outlined in IT Administrator/Special Access Policy (IT-XX).

SHSU accounts will have a unique identifier that is associated with a single user. Once an identifier is assigned to a particular person, it is always associated with that person. It is never subsequently reassigned to identify another person.

Use of the authentication service to identify oneself to an SHSU system constitutes an official identification of the user to the University, in the same way that presenting an ID card does. Security is everyone's responsibility, and everyone has a responsibility to protect their own "identity". Users will be held accountable for all actions of their account.

Regardless of the authentication method used, users must use only the authentication information that they have been authorized to use; i.e., must never identify themselves falsely as another person. Additionally, users must keep their authentication information confidential; i.e., must not knowingly or negligently make it available for use by an unauthorized person. Anyone suspecting that their authentication information has been compromised should contact the Information Security Office immediately.

Users must adhere to the requirements of the SHSU User Accounts Password Policy (IT-02).

SHSU Data Owners shall be responsible for ensuring that authorization and account management processes are documented and that the appropriate people have been assigned the responsibility of creating and maintaining authorization records.

SHSU Data Owners may monitor related activities of individuals as a condition for continued access. At a minimum, SHSU Data Owners must review user access privileges annually.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Intrusion Detection/Prevention and Security Monitoring Policy: IT-XX

PURPOSE:

The SHSU Information Security Office is charged with securing all SHSU owned information technology resources, both centralized and decentralized, and has the responsibility and university-wide authority to monitor the use of information technology resources to confirm that security practices and controls are in place, are effective, and are not being bypassed.

The purpose of the Intrusion Detection/Prevention and Security Monitoring Policy is to outline university policy regarding the monitoring, logging and retention of network packets that traverse SHSU networks, as well as observe events to identify problems with security policies, document existing threats and evaluate/prevent attacks.

Intrusion Detection and Prevention systems focus on identifying possible incidents, logging information about them, and reporting attempts to security administrators. It plays an important role in implementing and enforcing security policies.

SHSU takes reasonable measures to assure the integrity of private and confidential electronic information transported over its networks and to detect attempts to bypass the security mechanisms of information resources. This will allow for early detection of wrongdoing, new security vulnerabilities, or new unforeseen threats to information technology resources, thus minimizing the potential harmful impact.

SCOPE:

The Intrusion Detection/Prevention and Security Monitoring Policy applies to all individuals that are responsible for the installation of new information technology resources, the operation of existing information technology resources and individuals charged with information technology resource security.

POLICY STATEMENT:

SHSU considers all electronic information transported over the university network to have the potential to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as such.

While it is not the policy of SHSU to actively monitor internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the university's internet links. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by SHSU policies.

Audit logging, alarms and alert functions of operating systems, user accounting, application software, firewalls and other network perimeter access control systems will be enabled and reviewed annually. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Information Security Officer.

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- Local Area Network (LAN) traffic; protocols, and device inventory
- Operating system security parameters

The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Service desk trouble tickets and telephone call logs
- Network printer logs

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Operating system and software licenses

Any security issues discovered will be reported immediately to the Information Security Officer (ISO).

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Malicious Code Policy: IT-XX

PURPOSE:

This policy is intended to provide information to university information technology resource administrators and users to improve the resistance to, detection of, and recovery from the effects of malicious code.

SHSU information technology resources are strategic assets that, as property of the State of Texas, must be managed as valuable State resources. The integrity and continued operation of university information technology resources are critical to the operation of the University. Malicious code can disrupt normal operation of university information technology resources.

The number of information technology resource security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and decrease the cost of security incidents.

SCOPE:

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

This policy does not apply to approved academic programs where students develop and experiment with malicious programs.

POLICY STATEMENT:

The following requirements shall be adhered to at all times to ensure the protection of SHSU information technology resources:

<u>Prevention and Detection:</u>

- All desktops and laptops connected to the SHSU network must use SHSU approved virus protection software and configuration.
- Each file server attached to the SHSU network must utilize SHSU approved virus protection software and must be setup to detect and clean viruses that may infect file shares.

- Software to safeguard against malicious code (e.g. antivirus, anti-spyware, etc.) shall be installed and functioning on susceptible information technology resources that have access to the University network.
- All information technology resource users are prohibited from intentionally developing or experimenting with malicious programs (e.g. viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.) unless a part of an approved academic program.
- All information technology resource users are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.
- Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.
- Flash drives, external hard drives, and other mass storage devices will be scanned for malicious code before accessing any data on the media.
- Software safeguarding information technology resources against malicious code should not be disabled or bypassed by end-users.
- The settings for software that protect information technology resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of software that safeguards against malicious code should not be disabled, altered or bypassed by end-users to reduce the frequency of updates.

Response and Recovery:

- All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling service.
- If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current antivirus or other control software.
- If malicious code cannot be automatically quarantined or removed by antivirus software, the system should be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to Information Technology Services by contacting the Service Desk.
- Personnel responding to an incident should be given the necessary access privileges and authority to afford the necessary measures to contain/remove the infection.
- If possible, identify the source of the infection and the type of infection to prevent recurrence.
- Any removable media (including flash drives, external hard drives, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.
- IT@Sam Services personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information technology resources and submit to the Information

Security Officer to be included in the Department of Information Resources Security Incident Reporting System.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

IT Physical Access & Environmental Policy: IT-XX

PURPOSE:

This policy is intended to establish standards for securing IT@Sam data centers, network closets and protected IT facilities on the SHSU campuses. Effective implementation of this policy will minimize unauthorized access to these locations, provide more effective auditing of physical access controls and ensure environmental threats to IT@Sam data centers are monitored and remediated in a timely manner.

SCOPE:

The IT Physical Access Policy applies to IT@Sam data centers containing enterprise systems that serve the SHSU user community.

POLICY STATEMENT:

IT@Sam is responsible for the safety and security of data on the SHSU network and the equipment used to run the network infrastructure.

- Environmental conditions in all data centers will be monitored and protected from environmental threats commensurate with the identified risks and their importance to SHSU mission critical business processes.
- Physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all restricted information technology resource facilities must be documented and managed.
- All information technology resource facilities must be physically protected in proportion to the criticality or importance of their function at SHSU.
- Access to information technology resource facilities must be granted only to SHSU support personnel and contractors whose job responsibilities require access to that facility.
- The process of granting card and/or key access to information technology resource facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an information technology resource facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements

- Requests for physical access must come from IT@Sam.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the appropriate department. Keys or cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported immediately to the appropriate department.
- All information technology resource facilities that allow visitor access will track access with a sign in/out log.
- Visitors must be escorted in card access controlled areas of information technology resource facilities.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or not returned.
- Card access records and visitors logs for information technology resource facilities must be kept for routine review based upon the criticality of the information resources being protected.
- The person responsible for the information technology resource facility must promptly remove the card and/or key access rights of individuals that change roles within SHSU or are separated from their relationship with SHSU.
- The person responsible for the information technology resource facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the information technology resource facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Restricted access rooms should be identified with discrete signage.
-

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012

Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Portable Computing Policy: IT-XX

PURPOSE:

SHSU may, at its discretion, provide portable computing devices and media to employees. The portability offered by these devices and media increases the risk of unauthorized disclosure of information stored on them.

To maintain the confidentiality, integrity and availability of data and network resources at SHSU, the Portable Computing Policy establishes requirements for safeguarding electronic devices that can contain protected data.

SCOPE:

The SHSU Portable Computing Policy applies to all individuals that use portable computing devices and media, whether SHSU issued or privately owned, to access the SHSU information technology computing environment.

POLICY STATEMENT:

It is SHSU's policy to protect mobile computing devices and the information contained on such devices. Individuals that use these devices must ensure that they protect the hardware provided from theft and unnecessary damage as well as the data stored on them.

As a general practice, sensitive information should only be stored on servers. Data owners must carefully evaluate the risk of lost or stolen data against efficiencies related to mobile computing before approving the storage of confidential or sensitive information on portable computing devices.

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:

- Physically and logically safeguard the devices.
- Ensure that University-approved anti-malicious software applications and signatures are up-to-date.
- Use encryption to safeguard all storage media, (e.g., hard drives, USBs).
- Avoid unsecured or untrusted networks.
- Confidential information should not be accessed over unsecured or untrusted networks.
- Confidential information should not be stored on a portable computing device.

- Prevent the use of the portable computing device or media by unauthorized persons; are responsible for any misuse of the information by persons to whom they have given access.
- 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).
- Keep portable computing devices within view or securely stored at all times.
- Ensure the device is shut down or secured when not in use (e.g., password protect devices offering such capabilities).
- 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).
- Promptly notify IT@Sam if any portable computing device or media has been lost or stolen.

Requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. To address a specific circumstance or business need, the Chief Information Officer (CIO) may grant an exception to the encryption requirement for portable devices.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Privacy Policy: IT-XX

PURPOSE:

The purpose of the Privacy Policy is to clearly communicate privacy expectations to SHSU information technology resource users. It will define standards for managing and enforcing security on any information stored or passing through SHSU information technology resources or any personally owned or third-party device that may be connected to a state-owned resource.

Internal users 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 oversight. 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.

SCOPE:

The Internal Privacy Statements apply equally to all individuals who use SHSU information technology resources or connect personally-owned devices to SHSU information technology resources.

The Public Privacy Statements apply to members of the general public concerned about the types of information gathered and how that information is used.

POLICY STATEMENT:

<u>SHSU Internal Privacy:</u>

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of SHSU are the property of SHSU. These files are not private and may be accessed by authorized IT@Sam employees and campus administration at any time without knowledge of the information technology resource user or owner.

To manage systems and enforce security, IT@Sam may log, review and otherwise utilize any information stored on or passing through its information technology resource systems in accordance with the provisions and safeguards provided in the Texas Administrative Code § 202 (TAC § 202), Information Resource Standards. For these same purposes, IT@Sam may also capture user activity such as websites visited.

Third party and customer information has been entrusted to SHSU for business purposes and all faculty and staff will do their best to safeguard the privacy and security of this information. Customer account data is confidential and access will be strictly limited based on business need.

SHSU Website Public Privacy:

SHSU maintains the www.shsu.edu website and other SHSU-owned or –hosted domains as a public service. SHSU detailed public privacy statement is available on the website (IT-S02 – Web Privacy and Site Link) regarding individual websites, data collection, public forums, and links to other sites.

For site management functions, information is collected for analysis and statistical purposes (please refer to SHSU Web Privacy and Site Link Policy). This information is not reported or used in any manner that would reveal personally identifiable information unless SHSU is legally required to do so in connection with law enforcement investigations or other legal proceedings.

For site security purposes and to ensure that the site remains available to all users, SHSU uses software to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage which is strictly prohibited and may be punishable under applicable state and federal laws.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

System Development & Acquisition Policy: IT-XX

PURPOSE:

The purpose of the System Development & Acquisition Policy is to ensure that security is an integral part of SHSU system planning and management and the business processes associated with those systems.

It is important that the procedures for new and changed systems integrate information security requirements into the software life cycle of information systems that contain protected data. The security requirements must identify controls that are needed to ensure confidentiality, integrity, and availability. These controls must be appropriate, cost-effective, and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the protected data. This is true regardless of whether the systems are purchased, used from community or open source collaborations, or developed by SHSU.

SCOPE:

The System Development & Acquisition Policy applies to all software/systems installed and utilized on SHSU information technology resources that contain protected data.

This policy does not apply to approved academic programs where students develop and experiment with software programs.

POLICY STATEMENT:

All software developed in-house that runs on production systems shall be developed according to the IT@Sam Project Lifecycle and must adhere to the SHSU Application Security Policy (IT-XX). At a minimum, this plan shall address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and, post-implementation maintenance and review. The requirement for such methodology ensures the software will be adequately documented and tested before it is used for critical information.

Where resources permit, there shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Testing should not be done on live data due to the threat to its confidentiality and/or integrity.

All applicable systems shall have designated owners and custodians. Owners, and/or their designees, shall perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow testing of the system's security controls by SHSU, if needed. All acquired software that runs on production systems shall be subject to the IT@Sam Project Lifecycle and must adhere to the SHSU Application Security Policy (IT-XX).

An assessment of the system's security controls and a vulnerability assessment must be performed on all new enterprise information systems or ones undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production enterprise information systems and appropriate measures taken to address the risk associated with identified vulnerabilities.

The Change Management procedures will be followed to review and approve a change before it is moved into production.

Opportunities for information leakage should be appropriately minimized or prevented with risk assessments, monitoring and logs, and end-user awareness and training on preventive strategies.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX

Sam Houston State University

Information Technology Services (IT@Sam)

Third Party Access Policy: IT-XX

PURPOSE:

SHSU receives requests for direct connections to its information technology resources from contractors, vendors and other third parties for support services, contract work or other remote access solutions for university students, faculty, and staff.

The purpose of this policy is to define standards for connecting to SHSU information technology resources. These standards are designed to minimize the potential exposure to SHSU from damages which may result from unauthorized use of SHSU information technology resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical SHSU internal systems, etc.

SCOPE:

The Third Party Access Policy pertains to all third party organizations and individuals that require access to non-public electronic resources maintained by SHSU and who are not otherwise classified as full time, part time, or temporary faculty, staff, or students fall under this policy.

POLICY STATEMENT:

As a condition of gaining access to SHSU information technology resources:

- Every third-party must sign an SHSU Non-Disclosure Agreement.
- All third parties must be sponsored by an SHSU department, organization or employee.
- All third-party access must be uniquely identifiable and password management must comply with the User Accounts Password Policy (IT-02) and IT Administrator/Special Access Policy (IT-XX) guidelines.
- All third-party account holders must provide contact information that will be used to contact them in the event of account status changes, misuse, or termination of the agreement.
- All changes to access granted under this policy must originate from the SHSU sponsor and are subject to a security review.
- Third parties must be made aware and must comply with all applicable SHSU policies, practice standards, agreements and guidelines, including but not limited to:
    - Acceptable Use Policy (IT-03)
    - Encryption Policy (IT-10)

    - Privacy Policy (IT-XX)
    - Network Access Policy (IT-12)
    - Portable Computing Policy (IT-XX)
    - Privacy Policy (IT-XX)
    - Change Management Policy (IT-09)
    - Information Security Program
- Third-party agreements and contracts must specify:
    - The SHSU information to which the third party has access.
    - How SHSU information is to be protected by the third party.
    - Acceptable methods for the return, destruction or disposal of SHSU information in the third party's possession at the end of the contract.
- Third parties must only use SHSU information and information technology resources for the purpose of the business agreement.
- Any other SHSU information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others.
- Third-party personnel must report all security incidents immediately to the appropriate SHSU sponsor and the Information Security Officer (ISO).

Any third-party account holder that violates this policy will have the account suspended and the account holder's sponsor will be notified. Following a review, SHSU will implement the actions specified by the ISO to reinstate or remove the account.

Related Policies, References and Attachments:

An index of approved IT@Sam policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, XX, 2012
Next Review: November 1, 20XX