SHSU Faculty Senate
March 8, 2012
3:30 p.m. – 5:00 p.m.
LSC 304

Members Present:
Tracy Bilsing (CHSS), Len Breen (COE), Donald Bumpass (COBA), Erin Cassidy (NGL), Kevin Clifton (CFAMC), Donna Desforges (CHSS), Diane Dowdy (CHSS), Debbi Hatton (CHSS), Renee James (COS), William Jasper (COS), Gerald Kohers (COBA), Lawrence Kohn (COE), Paul Loeffler (COS), Sheryl Murphy-Manley (CFAMC), Tracy Steele (CHSS), Pamela Zelbst (COBA)

Members Not Present:
Jeff Crane (CHSS), Mark Frank (COBA), Randall Garner (CJ), Chad Hargrave (COS), Joyce McCauley (COE), Dwayne Pavelock (COS), Javier Pinell (CFAMC), Debbie Price (COE), Ricky White (COS), and Doug Ullrich (COS)

Visitors:
Ling Ren (CJ), Sofia Medrano of *The Houstonian* and Vice President of Finance, Al Hooten

Call to Order at 3:30pm

Approval of Minutes:
Unanih2 459.96 (n) -0.2.76cm BTm Tf [(U) -.2 (:) 0.2s (u) 0.2 -0.( ) 0.2 (R) -0.2 (i) (0.2 ( ) 0.2 (Pa Q q

Committee on Committees – Review of Annual Survey:
Gerald Kohers (chair, Committee on Committees) asked if Senators had any suggested changes to the annual faculty survey. It was agreed to remove questions 34 and 35 that relate to Blackboard and E-College respectively since both these LMS systems will soon be replaced (with replacement currently under review by the Senate). In regard to question 51 on the IDEA form, it was suggested that the question be split to address separate the issue of IDEA's accuracy and, separately, administering IDEA online. The proposed changes were passed unanimously and the survey will be distributed as amended by the committee.

University Affairs – IT Policies:
Erin Cassidy (chair, University Affairs Committee) reported that her committee had been asked by Mark Adams, Associate VP for IT, to review and comment upon seventeen IT policies (See the attached proposed policies and the committee's specific recommendations online). The Committee requested several clarifications including a definition of incidental use, what activities would jeopardize the university's tax exempt status, and the meaning of special access. In addition, the committee questioned what had happened to key cards to replace keys. In regard to the Malicious Code Policy, the issue of allowing access for approved students involved in course work or faculty involved in research on the topic was discussed – they should have access in specific cases only. The Senate unanimously approved the committee's recommendations and it will be sent on CAB with the Senate's questions and comments.

Chair's Report:
CoS Dean's Search:
The finalists are Robert Gannon (Valdosta State University), Neuropharmacology), Stanley Kelley (SHSU- Agricultural Sciences), and John Pascarella (Kansas State University – Biology). They hope to have a new Dean in place by the start of Fall 2012.

The CFAMC Dean's Search:
The search committee is still being formed. It is also hoped that that position will be filled by Fall of 2012.

DELTA:
DELTA would like to place offices for one staff member in academic buildings (to improve service to faculty). DELTA will be moved to the old Residence Life building.

March to the Grave:
On Friday, March 2, there was a report of gun incident in Huntsville. In fact, the Walter P. Webb Society (essentially the History Club for SHSU) was marking the birthday of Sam Houston with a march to his grave which included students dressing in period costumes and carrying inoperable replica guns. It was a false alarm.

LMS Survey:
Paul Loeffler (chair, Faculty Affairs Committee), reported that the committee has been working closely with DELTA. So far Blackboard 9 and Canvas were the two favorites. It was confirmed that DELTA will recommend for adoption whatever the committee and the Senate decides.

A significant issue facing SHSU is fees (he described it as the first curveball). Just yesterday Mr. Hooten was informed that request for fee increases must be limited. It has now been determined that universities in our system may only request fee increases for two periods. First, fee increase requests may be made in Spring 2013 and,

In regard to increasing efficiency at SHSU we have created an organization and efficiency committee. Mr. Hooten reported that his previous institution had enacted changes that allowed them to save $1.4 million per year through a similar process. SHSU is presently conducting a survey (call for recommendations on efficiency) that it is hoped will produce similar results.

Mr. Hooten informed the Senate that there may be a move (originating from the current president of TAMU) to privatize including building and custodial maintenance.

Finally, there was a discussion of indirect costs of grants.

New Business:
None

Adjourned at 5:00pm

REPORT ON CLINICAL FACULTY MEMBERS

The Academic Affairs Committee has determined that the confusion over clinical faculty rights and responsibilities stems largely from a lack of communication. Also, there is a problem in the wording of the Academic Policy specifically addressing Clinical Faculty. We make the following recommendations to fix these issues.

First, the problem of reapplying on a yearly basis is widespread, and results from poor communication. While the appointment is annual (as per Section 3.02 of Academic Policy 041020), the application process is not:

"3.02 The duration of each appointment will be for one year. Additional one-year appointments may be made at the discretion of the University, and no property right in the title shall be conferred by virtue of this appointment. Appointment renewal will be contingent upon the University's sole judgment as to the quality and level of service provided by the clinical faculty member to the University."

IT IS IMPORTANT TO NOTE THAT CLINICAL FACULTY MEMBERS DO NOT HAVE TO REAPPLY EACH YEAR, only that the appointment itself is made on an annual basis. It is also important to note that clinical faculty members have the right to renegotiate their appointments on an annual basis, allowing them to be promoted (e.g. from Clinical Assistant Professor to Clinical Associate Professor), seek pay raises, and redefine their roles.

We propose that a formal recommendation be made to Provost Hebert to clarify this point for all Deans, Department Chairs, and others involved in the hiring and appointing process.

Also, there are two sections in the Academic Policy that appear to be in direct conflict with each other, namely 4.02e, which states:

"e. Voting and Other Rights. The proposal shall define the rights and responsibilities of appointees in the proposed titles, including their voting status in their respective department/school and/or college, and their access to grievance and appeals processes available to tenure-track faculty"

And 5.01, which states:

"5.01 During their term of service, clinical faculty members shall be accorded the same privileges and perquisites at the University as tenure-track faculty."

WE PROPOSE THE FOLLOWING CHANGE BE MADE TO 5.01 TO BRING IT IN LINE WITH THE UNDERSTOOD FUNCTION OF CLINICAL FACULTY:

5.01: During their term of service, clinical faculty members shall be accorded privileges and perquisites as agreed upon in their annual contracts.

Sam Houston State University
Exemptions & Waivers
2007 thru 2011

Exemptions	2011	2010	2009	2008	2007
Hazelwood	1,434,067.49	681,396.28	437,200.10	393,614.30	353,781.00
Firemen (Children of Disabled Firefighters/Law Enforcement Officers)	15,830.00	30,912.00	17,619.50	5,729.00	22,519.00
Dual Enrollment	0.00	0.00	0.00	0.00	0.00
Thesis	0.00	0.00	0.00	0.00	0.00
Blind & Deaf	174,880.50	161,511.74	151,470.50	141,587.00	131,421.50
Valedictorian	69,112.00	81,840.00	69,508.00	43,014.00	63,960.00
Foster Children	253,442.00	217,214.75	138,214.95	127,135.90	90,080.30
Disabled Peace Officers	0.00	0.00	0.00	1,034.10	0.00
Texas Tomorrow Fund	8,353.74	10,050.70	5,212.12	2,789.12	2,880.01
Distance Learning	694,488.00	950,253.12	674,375.70	517,202.74	393,791.30
Seniors 65 and over	978.00	1,960.00	0.00	1,800.00	1,260.00
Children or Spouse of Deceased Public Servant	6,353.00	6,514.50	0.00	0.00	0.00
Preceptor	1,500.00	600.00	3,350.00	2,050.00	0.00
Total Exemptions	2,659,004.73	2,142,253.09	1,496,950.87	1,235,956.16	1,059,693.11
Waivers					
Good Neighbor	10,920.00	17,958.00	31,762.00	19,288.00	3,300.00
Common Market	0.00	0.00	0.00	0.00	0.00
Employee Exempt	520,117.20	485,720.21	329,322.90	436,589.97	451,127.60
Academic Scholarship Exempt	1,537,755.00	1,475,856.00	1,289,386.50	1,020,306.60	828,301.00
Military Exempt	13,640.00	18,005.00	46,365.00	135,664.00	104,362.50
Employee Spouse (Faculty and Dependents)	0.00	7,202.00	8,711.00	20,306.60	29,150.00
Economic Dev & Diversification	8,370.00	9,141.00	9,554.00	0.00	

Sam Houston State University
Exemptions & Waivers
Fiscal Year 2008

EXEMPTIONS	Unduplicated Count	Education & General Funds	Designated Funds	Auxiliary Funds	Totals
Hazelwood	146	107,567.00	262,858.65	23,188.65	393,614.30

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:

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,

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

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 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.

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

unauthorized users to access the network. The university is bound by its contractual and license agreements respecting certain third-

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 fede

2. Applications installed or being changed should follow the standardized

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

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

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

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.

which may follow from unaut

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:

- .

malicious by the university's

ating SHSU firewall policies is

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

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

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/Prevent(/)logging information about them, and reporting atter
plays an important role in implementing and enforcing security

SHSU takes reasonable measures to assure the integrity of privat

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

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

- 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.
-

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

In

- 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

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

The users of portable computing devices

- 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

Sam Houston State University

Information Technology Services (IT@Sam)

System Development & Acquisition Policy: IT-XX

PURPOSE:

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 crit

- Privacy Policy

!"#$%&'()#*+,'+-#.#/0',+12'3)#4556'12#7%8 8'33++9#:;1'0<#=>?=#
#

@%1#3A+#8%23#;6139#3A+2+#;%&'('+2#B%(C8+03#;16(3'(+2#6&1+6B)#'0#;&6(+#60B#6&1+6B)#C0B+123%%B#D%1#
C0B+12360B6E&+F#E)#8%23#+8;&%)++2G#8%23#61+#E62+B#'0#(%8 8%0#(%1;%163+#0+3-%1H#2+(C1'3)#;16(3'(+2I#
J A+1+#6;;&'(6E&+9#;%&'('+2#A6,+#E++0#-%1B+B#3%#6&&%-#+K(+;3'%02#5%1#6;;1%,+B#1+2+61(A#60B#2'8'&61#
6(3',3'+2#DE)#E%3A#56(C&3)#60B#23CB+032FI# J A+1+#6;;&'(6E&+9#;%&'('+2#'0(&CB+#<C'B+&'0+2#5%1#5C3C1+#1+,'+-#
%5#;%&'('+2#'0#H++;'0<#-'3A#(A60<'0<#2)23+82#60B#0++B2I#"A+1+#61+#(%0(+102#1+<61B'0<#;%%1#<16 8 861#'0#
2%8+#;%&'('+29#-A'(A#2A%C&B#E+#(%11+(3+B#;1'%1#3%#;CE&'(#;%23'0<#%5#3A+#;%&'('+2I##
#

#

?I L+B'6#:60'3'M63'%O#$%&'()N# #

#

=I O%0PQ'2(&%2C1+#4<1++8+03#$%&'()N# #

#

RI *'2H#422+228+03#$%&'()#.# #

- $%&'()#:363+8+039#1%&+#%5#3A+#Q636#S-0+1N#8%,+#3A+#-%1B#T60BU#51%8#3A+#+0B#%5#3A+#5'06&#EC&&+3#'3+8 9#60B#'023+6B#;&6(+#'3#63#3A+#+0B#%5#3A+#2+(%0BP3%P&623#EC&&+3#'3+8 I#
- $%&'()#:363+8+039#1%&+#%5#3A+#!O5%1 8 63'%0#:+(C1'3)#S55'(+19#EC&&+3#VRN#"A'2#2363+8+03#2A%C&B#E+<'0#-'3A#TW+U#'0#;&6(+#%5#T!29U#2'0(+#3A+#;1+(+B'0<#2+03+0(+#2363+2#3A63#T"A+#!:SX#2A6&&NU#
  #

YI 4((+;36E&+#/2+#$%&'()#

.# !

##

- 7&61'5'(63'%O2N#
  - *+231'(3'%09#EC&&+3#?PBI## J A63#(%023'3C3+2#T'0('B+036&#C2+ZU#S0+#(60#+0,'2'%0#3A'2#-%1B'0<#B+&'E+163+&)#E+'0<#C2+B#;C0'3',+&)#6<6'023#2%8+%0+#BC+#3%#%;+00+22#3%#'03+1;1+363'%0I#$+1A6;2#'0(&CB+#B'(3'%061)#B+5'0'3'%0#%5#T'0('B+036&UZ##
  - *+231'(3'%029#EC&&+3#VYN#!0(&CB+#+K68;&+2#%5#T4(3',3'+2#3A63#-%C&B#[+%;61B'M+#3A+#

aI !"#4B8'0'23163%1^:;+('6&#4((+22#$%&'()#.#

?YI $%136E&+#7%8 ; C3'O<#$%&'()#.# #

#

?aI $1',6()#$%&'()