

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

**Policy Compliance: IT-00**

**Purpose**

SHSU's information services network has been established for the use and benefit of SHSU in the conduct of its academic, business, and other operations. This document provides an index of all university-wide policies for the Office of Information Technology Services as well as common elements of privacy, enforcement, legal reference and definitions.

**Privacy**

Because of its stated purposes, SHSU's information services network is not a "public forum" for purposes of freedom of speech or other First Amendment activity. Moreover, anyone using the network should have no expectation of privacy and should not expect to be free from access, by the University to and any and all information entered into, assembled, or otherwise maintain on such network.

SHSU's information resources are subject to review and disclosure in accordance with:

1. The Texas Public Information Act, the federal Freedom of Information Act, and other related laws, Regents' Rules, and university policies;
2. Other policies or legal requirements, such as subpoenas and court orders;
3. Efforts to protect and sustain their operational performance and integrity;
4. Security reviews, audits, and investigations by authorized individuals in the performance of their assigned duties;
5. Monitoring to assure that the network has not been misused; and,
6. Such other purposes as the University, in its sole discretion, judges necessary to protect its own best interests and/ or those of other users.

Anyone using SHSU's information resources expressly consents to university monitoring of the network at any time and for any purpose, including but not necessarily limited to, evidence of possible criminal activity, violations of law, contract, copyright or patent infringement, and/or violation of any university or Texas State University System policy, rule, or regulation.

Further, all users should understand that, while the university takes reasonable precautions, it cannot guarantee the protection of electronic files, data, or e-mails from unauthorized or inappropriate access. Users should not expect privacy from disclosure in any messages or other use of Texas State's information resources.

**Violations**

Violation of University policy may result in disciplinary action which may include termination of employment for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Sam Houston State University Information Resources access privileges, civil, and criminal prosecution.

### **Obtaining a Policy Exemption**

Exemptions are granted on a case-by-case basis and must be reviewed and approved by the University designated IRM. The IRM will mandate the documentation and additional administrative approvals required for consideration of each policy exemption request.

### **Approved Policy Index:**

#### **Approved by Cabinet 27 June 2011 with TSUS Legal review finalized 28 July 2011**

- IT-01 User Accounts Management Policy  
Regular Review Date: November, Odd Number Years
- IT-02 User Accounts Password Policy  
Regular Review Date: November, Even Number Years
- IT-03 Acceptable Use Policy  
Regular Review Date: November, Odd Number Years
- IT-04 VPN Access Policy  
Regular Review Date: November, Even Number Years
- IT-05 Data Access Review Policy  
Regular Review Date: November, Odd Number Years
- IT-06 Data Classification Policy  
Regular Review Date: November, Even Number Years
- IT-07 Technology Incident Management Policy  
Regular Review Date: November, Odd Number Years
- IT-08 System Development Policy  
Regular Review Date: November, Even Number Years
- IT-09 Information Technology Change Management Policy  
Regular Review Date: November, Odd Number Years
- IT-10 Digital Storage Policy  
Regular Review Date: November, Even Number Years
- IT-11 Data Backup Policy  
Regular Review Date: November, Odd Number Years
- IT-12 Network Use and Vulnerability Assessment Policy  
Regular Review Date: November, Even Number Years
- IT-13 Security Training Policy  
Regular Review Date: November, Odd Number Years
- IT-14 Server Administration Policy  
Regular Review Date: November, Even Number Years

## Reference

In addition to the general principles set forth in this policy statement, the use of information technology resources may be affected by a number of other legal requirements and ethical principles. While it is not possible to list all potentially applicable laws and regulations, the most relevant to the use of institutional information technology resources are listed in TSUS Policy Guideline TSUS IT.02.01, Information Security Policy, and are included in this policy guideline by reference. The primary applicable references sources follow:

1. Guidelines of the Texas Department of Information Resources
  - a. IRM Act, 2054.075(b)
  - b. DIR Practices for Protecting Information Resources Assets
  - c. DIR Standards Review and Recommendations Publications
2. Statutes pertaining to the use of university information resources include the following:
  - a. The Federal Family Educational Rights and Privacy Act (FERPA) – restricts access to personally-identifiable information from students' education records.
  - b. Texas Administrative Code, Title 1, Part 10, Chapter 202 – Regulations from the Department of Information Resources establishing information security requirements for Texas state agencies and higher education institutions.
  - c. Texas Penal Code, Chapter 33: Computer Crimes – Texas law pertaining to computer crimes. This statute specifically prohibits unauthorized use of university computers, unauthorized access to stored data, or dissemination of passwords or other confidential information to facilitate unauthorized access to the university's computer system or data.
  - d. Texas Penal Code, §37.10: Tampering with Governmental Record – Prohibits any alteration, destruction, or false entry of data that impairs the validity, legibility or availability of any record maintained by the university.
  - e. United States Code, Title 18, Chapter 47, § 1030: Fraud and Related Activity in Connection with Computers – Federal law specifically pertaining to computer crimes. Among other stipulations, prohibits unauthorized and fraudulent access to information resources, accessing a computer to obtain restricted information without authorization; altering, damaging, or destroying information on a government computer without authorization; trafficking in passwords or similar information used to gain unauthorized access to a government computer; and transmitting viruses and other malicious software.
  - f. Copyright Act of 1976 – Federal law that forms the primary basis of copyright law in the United States, as amended by subsequent legislation. The Act spells out the basic rights of copyright holders, codifies the doctrine of "fair use," and for most new copyrights, adopts a unitary ownership period based on the date of the author's death rather than the prior scheme of fixed initial and renewal terms.
  - g. Digital Millennium Copyright Act (DMCA) – Signed into law on October 20, 1998, as Public Law 105-304. Created to address the digitally networked environment, the DMCA implements the World Intellectual Property Organization (WIPO) Internet Treaties; establishes safe harbors for online service providers; permits temporary copies of programs during the

performance of computer maintenance; and makes miscellaneous amendments to the Copyright Act, including amendments that facilitate Internet broadcasting.

- h. Electronic Communications Privacy Act (U.S.C., Title 18) – Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.
- i. Computer Software Rental Amendments Act of 1990 – Deals with the unauthorized rental, lease, or lending of copyrighted software.
- j. Texas Government Code §556.004 – Prohibits using state resources or programs to influence elections or to achieve any other political purpose.
- k. Health Insurance Portability and Accountability Act (HIPAA) – Public Law 104-191, August 21, 1996. The final standards were published in February, 2003 and emphasize security management principles and broad management controls as primary vehicles for protecting patient health information. HIPAA was enhanced in 2009 by the HITECH Act, which extended HIPAA's provisions to the business associates of covered entities and imposed new notification requirements on covered entities, their business associates, and the vendors of personal health records for breaches of protected health information.
- l. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, Public Law 107-296 – Required every federal agency to develop, document, and implement an agency-wide information security program. The law was amended by FISMA 2010, which changed the focus from paperwork compliance to continuous monitoring and threat mitigation.
- m. Security Configuration Benchmarks published by the Center for Internet Security (CIS). CIS Benchmarks are provided for a wide array of operating systems, application software, and multiple versions thereof. CIS Benchmarks are defined via consensus among security professionals worldwide and used by thousands of enterprises as their de facto local configuration standards.

## Definitions

**1. Data Owners:** Data Owners are those who, by virtue of their position at SHSU, have the authority to appoint data custodians. As such they have ultimate responsibility for the security, accuracy and confidentiality of data within their areas of accountability. Data Owners generally will delegate responsibility to Data Custodians for the management of data (including granting inquiry, entry and update data privileges, and defining business processes.) The responsibility for maintaining and controlling Banner validation and rules tables resides with the Data Owners. Data Owners must review all denials for data access and affirm or override the denial decision prior to user notification. It is expected that Data Owners will be ex-officio members of the Data Standards Committee. **SHSU**

### **Data Owners:**

- a. Finance and Operations, VP Finance and Operations
- b. Student and Enrollment Management, VP Enrollment Management

- c. Academic Affairs, Associate Provost
- d. Banner General, Designated IRM

2. **Data Custodians:** A Data Custodian is the individual designated by the Data Owner to be responsible for management of data. Each Data Custodian is automatically a member of the Data Standards Committee. The Data Custodian may make data within his/her charge available to others for the use and support of the office or department's functions. Before granting access to data, the Data Custodian must be satisfied that protection requirements have been implemented and that a "need to know" is clearly demonstrated. By approving user access to SHSU data, the Data Custodian consents to the use of that data within the normal business functions of administrative and academic offices or departments. Data Custodians are responsible for the accuracy and completeness of data files in their areas. Misuse or inappropriate use by individuals will result in revocation of the user's access privileges. Data Owners are also responsible for the maintenance and control of Banner validation and rules tables. These tables, and processes related to their use, define how business is conducted at SHSU. **SHSU Data Custodians:**

- a. Graduate Admissions: Director of Projects
  - b. Undergraduate Admissions: Director
  - c. Purchasing: Director of Procurement and Business Services
  - d. Budgeting: AVP Budget and Operations
  - e. Student Records: Registrar
  - f. Banner General: Director ERP Services
  - g. Financial Aid: Director of Financial Aid
  - h. Residence Life: Director of Residence Life
  - i. Human Resources: Director of Human Resources
  - j. Payroll: Manager
  - k. Accounting, Cashier, Accounts Payable: Controller
3. **Development system** – An SHSU maintained system or service which is used to test changes to code, processes, or system operation prior to modifying the corresponding Production system or service.
4. **Downtime** – Downtimes constitute any interruption in service or loss of functionality.
5. **Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
6. **Information Resources Manager (IRM):** Responsible to the State of Texas for management of the agency's information resources. The designation of an

agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

7. **Information Security Officer (ISO):** Responsible to the executive management for administering the information security function within the agency. The ISO is the agency's internal and external point of contact for all information security matters.
8. **Maintenance:** Changes to or work performed on a system or service which could result in a service interruption or which presents a significant change to service functionality.
9. **Production system:** An SHSU maintained system or service which is used by students, faculty, staff, or the public for critical day-to-day business operations of the University.
10. **Server Owner:** Server Owners are responsible for establishing server usage policies, specifying server access controls (both physical and electronic), and assuring compliance with state and institutional server management standards.
11. **Server Administrator:** Server Administrators are responsible for enforcing the owner's usage policies, implementing the owner-specified access controls, and configuring and maintaining the server according to the required standards.
12. **User:** An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.