Sam Houston State University
A Member of The Texas State University System
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 information technology resources that are 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 as determined by supervisor; or,
   e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.
2. Allowing 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 can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2015