

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

Acceptable Use Policy: IT-03

Introduction:

The SHSU Network and other information technology resources at SHSU are shared among community members. The SHSU Acceptable Use Policy is intended to help members of the SHSU community use SHSU's computing and network facilities responsibly, safely, and efficiently thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities and assure that all use of them is responsible, legal, and respectful of privacy.

Laws that apply in "the real world" also apply in the "virtual" networked computer world (including the SHSU Network). Laws about libel, harassment, privacy, copyright, stealing, threats etc. are not suspended for computer users, but apply to all members of society whatever medium they happen to be using including face-to-face, phone, computers and other electronic media equipment. Furthermore, law-enforcement officials vigorously prosecute cyber related violations of the law.

Scope:

The SHSU Acceptable Use policy applies equally to all individuals utilizing SHSU information technology resources.

Policy Statement:

It is important to understand the purpose of the SHSU network so that your use of the system is in compliance with that purpose. The purpose of the SHSU network is 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 computer must adhere to all the same policies that apply to use from within SHSU facilities.

Employees must not allow family members with no SHSU affiliation or other non-employees to access SHSU password protected computer systems.

Direct violations of the intended use of the SHSU network include the following:

1. Interfering or altering the integrity of the system at large by:
 - a. Permitting another individual to use your user account;
 - b. Impersonating other individuals in communication;
 - c. Attempting to capture or crack passwords or encryption;
 - d. Unauthorized access, destruction or alteration of data or programs belonging to other users; or
 - e. Restricting or denying access to the system by legitimate users.

2. Using the SHSU network for private financial gain or personal benefit. Users are not permitted to run a private business on any state resource including the SHSU network. Commercial activity is permitted but only for business done on behalf of SHSU or its organizations.
3. Transmitting threatening or harassing materials. You must not intentionally access, create, store or transmit 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).
4. Not reporting any weaknesses in SHSU computer security or any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the university-designated IRM.
5. Attempting to access any data or programs contained on SHSU systems for which you do not have authorization or explicit consent.
6. Sharing your SHSU accounts, passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
7. Making unauthorized copies of copyrighted material.
8. Using shareware or freeware software without SHSU IT@SAM management approval unless it is on the SHSU standard software list.
9. Degrade the performance of information technology services; deprive an authorized SHSU user access to a SHSU resource; obtain extra resources beyond those allocated; circumvent SHSU computer security measures.
10. 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.
11. 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, May 15, 2011
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2013