IT-03: Acceptable Use Policy

Summary

This policy covers what is acceptable use of university information resources.

Body

PURPOSE

The information resources at Sam Houston State University (SHSU) support the academic, 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 information resource 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 resources.

Pursuant to Texas State University System Rules and Regulations Chapter III, Paragraph 19, this document establishes specific requirements for the use of all information resources at SHSU.

SCOPE

This SHSU Acceptable Use policy applies equally to all individuals utilizing SHSU information resources, including but not limited to SHSU employees, faculty, students, alumni, agents, consultants, contractors, volunteers, vendors, temps, visitors, etc.

Information 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 device connected to the network or accessing SHSU information.

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 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.

ACCEPTABLE USE

The SHSU network exists to support academic, research, 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.

1. Access to SHSU information resources from any device must adhere to all the same policies that apply to use from within SHSU facilities.
2. Users may use only SHSU information resources for which they are authorized.

3. 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 SHSU 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 resources.
4. Users should secure resources against unauthorized use or access to include SHSU accounts, passwords, Personal Identification Numbers (PIN), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes.
5. Users must report all software 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 or through another pre-approved means of disclosure (e.g., Passman).
6. Users must not attempt to access SHSU information resources without appropriate authorization by the system owner or administrator.

RESTRICTIONS

All individuals are accountable for their actions relating to SHSU information resources. Direct violations include the following:

1. Interfering or altering the integrity of SHSU information resources by:
    - Impersonating other individuals in communication;
    - Attempting to capture or crack passwords or encryption;
    - Unauthorized access, destruction, or alteration of data or programs belonging to other users;
    - Excessive use for personal purposes, meaning use that exceeds incidental use as determined by IT@Sam; 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 resources.
3. Using the SHSU information resources for private financial gain or personal benefit. Users are not permitted to run a private business on any SHSU information 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 resources for political purpose.
6. Using SHSU information resources to threaten or harass others in violation of the Texas State University System (TSUS) *Rules and Regulations, Chapter V, Paragraphs 2.4* or *4.51*.
7. Intentionally accessing, creating, storing or transmitting illegal material.
8. Not reporting any weaknesses in SHSU information 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 resources for which authorization has not been given.
10. Making unauthorized copies of copyrighted material.
11. Degrading the performance of SHSU information resources; depriving an authorized SHSU user access to an SHSU information resource; obtaining extra information resources beyond those allocated; or circumventing SHSU security measures.
12. Possessing, downloading, installing, or running security programs, utilities, or devices that reveal or exploit weaknesses in the security of an information resources. For example, SHSU users must not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on SHSU information resources.
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 TSUS.

REFERENCE

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the TSUS Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version: 1.02
Approved By: President’s Cabinet, April 11, 2023
Reviewed By: Heather Thielemann, Information Resources Manager, April, 2023
Next Review: April, 2024