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

Authorized Software Policy: IT-19

PURPOSE:

Authorized software is any software that is acceptable for use on Sam Houston State University (SHSU) information resources. The purpose of the Authorized Software Policy is to provide a set of measures that will mitigate information security risks associated with authorized software.

SHSU has negotiated special pricing and licensing for a variety of software available to students, faculty, and staff. Other software is readily available in the open marketplace under a licensing agreement. When software poses a security threat to SHSU, its use may be restricted.

Users entrusted with SHSU information resources are responsible for maintaining licensing information for any software the user installs, and if requested by the University, must provide SHSU with that licensing information. This includes, but is not limited to, smart phones, tablets, laptops, etc.

Non-compliance with copyright laws regarding software is subject to civil and criminal penalties imposed by federal and state laws. These penalties are applicable to the University and/or an individual.

SCOPE:

The Authorized Software Policy applies to all users of SHSU information resources.

POLICY STATEMENT:

1. All software installed or used on SHSU-owned information resources must be appropriately licensed. IT shall maintain sufficient documentation to validate that the software is appropriately licensed.

2. Persons installing or authorizing the installation of software should be familiar with the terms of the license agreement.

3. Users are responsible for preventing illegal software usage and abides by university policy on the use of copyrighted materials. These responsibilities include:

    a. Do not illegally distribute or share software with anyone.
    b. Ensure all software is license compliant, including personally purchased software.
    c. Ensure all software licenses are readily available.

d. Report any suspected or known misuse of software to IT@Sam Service Desk.

4. The following general categories of software are specifically prohibited on all SHSU information resources unless specifically authorized by the Information Security Officer:

    a. Software used to compromise the security or integrity of computer networks and security controls such as hacking tools, password descramblers, network sniffers, and port scanners.
    b. Software that proxies the authority of one user for another, for the purpose of gaining access to systems, applications, or data illegally.
    c. Software which instructs or enables the user to bypass normal security controls.
    d. Software which instructs or enables the user to participate in any activity considered a threat to local, state, or national security, including the assistance or transfer of information leading to terrorist activity or construction or possession of illegal weapons.
    e. Any other software specifically prohibited by the Information Security Officer.

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 Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, May, 2023
Next Review: May, 2024