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

Portable Computing Policy: IT-26

PURPOSE:

Sam Houston State University (SHSU) may, at its discretion, provide or allow use of portable information resources (portable devices) including communication and/or storage Devices (e.g., laptops, tablets, flash drives, removable hard drives, optical disks) to access SHSU information resources. While mobility offers these devices increased usefulness and convenience, it also increases the risk of theft, information loss, or unauthorized disclosure of information to SHSU.

To maintain the confidentiality, integrity, and availability of information resources at SHSU, the Portable Computing Policy establishes requirements for safeguarding portable devices.

SCOPE:

The SHSU Portable Computing Policy applies to all individuals who use portable devices, whether SHSU issued or privately owned, which may store, transmit, or process protected or confidential SHSU information or are used to access other SHSU information resources.

POLICY STATEMENT:

1. Information owners must carefully evaluate the risk of lost or stolen data against efficiencies related to mobility before approving portable devices usage with SHSU information.

2. The users of portable devices are expected to take all appropriate measures and precautions to prevent the loss, theft, damage and/or unauthorized use and shall include the following:

    a. Physically and logically safeguard the portable device.

    b. Ensure that University-approved security applications are in use and signatures are up to date.

    c. Install only vendor-supported Operating Systems and applications and keep them up to date with the latest security updates.

    d. Encrypt SHSU information stored on portable devices.

    e. Avoid connecting portable devices to unsecured or untrusted networks or equipment.

    f. Use only secure communications protocols (e.g., secure web browsing using HTTPS).

g. Prevent the use of the portable device by unauthorized individuals; users are responsible for any misuse of the portable device by unauthorized individuals to whom they have given access.

h. All reasonable precautions to prevent unauthorized information disclosure should be taken when using portable devices including but not limited to:

    i. shielding screen from passive viewing,
    ii. enabling a screen saver or home screen lock,
    iii. using headphones to listen to audio

i. Keep portable devices within view or securely stored at all times.

j. Ensure the portable device is shut down or secured when not in use (e.g., password protect devices offering such capabilities).

k. Unattended portable devices must be physically secure (e.g., locked in an office, desk drawer or filing cabinet). If secured in an automobile, keep the portable device in a non-visible location and remove it as soon as possible (to avoid heat damage or theft).

l. Promptly notify IT if any portable computing device or media has been lost or stolen.

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, June, 2023

Next Review: June, 2024