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

Portable Computing Policy: IT-26

PURPOSE:

SHSU may, at its discretion, provide portable computing devices and media to employees. The portability offered by these devices and media increases the risk of unauthorized disclosure of information stored on them.

To maintain the confidentiality, integrity and availability of data and network resources at SHSU, the Portable Computing Policy establishes requirements for safeguarding electronic devices that can contain protected data.

SCOPE:

The SHSU Portable Computing Policy applies to all individuals that use portable computing devices and media, whether SHSU issued or privately owned, to access the SHSU information technology computing environment.

POLICY STATEMENT:

It is SHSU's policy to protect mobile computing devices and the information contained on such devices. Individuals that use these devices must ensure that they protect the hardware provided from theft and unnecessary damage as well as the data stored on them.

As a general practice, sensitive information should only be stored on servers. Data owners must carefully evaluate the risk of lost or stolen data against efficiencies related to mobile computing before approving the storage of confidential or sensitive information on portable computing devices.

The users of portable computing devices or media used to store, transmit or process protected data are expected to take all appropriate measures and precautions to prevent the loss, theft, damage and/or unauthorized use and shall include the following:

- Physically and logically safeguard the devices.
- Ensure that University-approved anti-malicious software applications and signatures are up-to-date.
- Use encryption to safeguard all storage media, (e.g., hard drives, USBs).
- Avoid unsecured or untrusted networks.
- Confidential information should not be accessed over unsecured or untrusted networks.
- Confidential information should not be stored on a portable computing device.

- Prevent the use of the portable computing device or media by unauthorized persons; are responsible for any misuse of the information by persons to whom they have given access.
- All reasonable precautions to prevent data compromise should be taken when using portable computing devices (e.g., shield screen from passive viewing, password protected screen saver).
- Keep portable computing devices within view or securely stored at all times.
- Ensure the device is shut down or secured when not in use (e.g., password protect devices offering such capabilities).
- Unattended portable computing devices must be physically secure (e.g., locked in an office, desk drawer or filing cabinet; in an automobile, secure in a non-visible location).
- Promptly notify IT@Sam if any portable computing device or media has been lost or stolen.

Requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. To address a specific circumstance or business need, the Chief Information Officer (CIO) may grant an exception to the encryption requirement for portable devices.

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, 2014