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

Media Sanitization Policy: IT-15

PURPOSE:

It is the policy of Sam Houston State University (SHSU) that all data must be removed from devices and equipment that are capable of data storage, transmission or receipt prior to equipment disposal.

Technical support staff will properly sanitize information technology resources prior to transfer, sale or disposal. It is imperative that all devices capable of storing SHSU information be sanitized in a way that will make data recovery impossible.

This document establishes specific requirements for Information Technology media sanitization at Sam Houston State University. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202) and TSUS Rules and Regulations; Chapter III, Paragraph 19)

SCOPE:

The SHSU Media Sanitization Policy applies to any data owner, data custodian, system administrator and OITS staff that installs, operates or maintains SHSU information technology resources.

POLICY STATEMENT:

Prior to the sale, transfer or disposal of information technology resources, the technical support staff will take the appropriate steps, per the IT@Sam Property Office Media Sanitization Procedures, to ensure all data is removed from any associated storage device.

1. Information technology resources shall be sanitized utilizing a method that will ensure data recovery is impossible, such as degaussing, shredding, or destroying the media utilizing a destruction method that will be able to withstand a laboratory attack (e.g., disintegration, pulverization, melting or incineration).

2. If the device is a cell phone or PDA remove subscriber identity module (SIM) and additional memory cards and destroy per sanitization requirements. Sanitize the unit utilizing a method that will ensure data recovery is impossible.

3. Document the removal and completion of the process with the following information:

    a. Date;

b. Description of the item(s) and serial number(s);
c. Inventory number(s);
d. The process and sanitization tools used to remove the data, or process and method used to for destruction of the media; and
e. The name and address of the organization to which the equipment was transferred, if applicable.

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, December 15, 2011
Approved by: President's Cabinet, January 9, 2012
Next Review: November 1, 2015