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

Media Sanitization Policy: IT-15

PURPOSE:

Technical support staff will properly sanitize information 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 media sanitization at Sam Houston State University (SHSU).

SCOPE:

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

POLICY STATEMENT:

1. All SHSU data must be removed from all information resources (devices, equipment, memory cards, etc.) that are capable of data storage, transmission or receipt prior to device and equipment sale, transfer, or disposal.

2. Information 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).

3. Document the removal and completion of the sanitization 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 for destruction of the media; and
    e. The name and address of the organization to which the equipment was transferred, if applicable.

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, May 2, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, May, 2023
Next Review: May, 2024