

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

**Digital Storage Policy: IT-10**

**Introduction:**

Digital storage devices can provide massive storage for the SHSU community. These devices, however, carry additional responsibilities for maximizing reliability, efficient management, and security. If licensed software programs and/or confidential institutional data (as referenced in IT@SAM policy IT-06) are stored on digital storage devices, the information must be encrypted while needed and completely erased and/or destroyed before the device is transferred out of University control or erased before being transferred from one University department or individual to another. Sam Houston State University is committed to compliance with federal statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements.

All constituents of Sam Houston State University have a responsibility to ensure the confidentiality of federally regulated and otherwise protected sensitive or proprietary information residing on University-owned computer systems and other digital storage devices and media.

**Scope:**

The SHSU External Digital Storage policy applies equally to all individuals granted access privileges to any Sam Houston State University information technology resources.

**Policy Statement:**

All computers and digital storage devices including, but not limited to desktop workstations, laptops, servers, notebooks, and handheld computer hard drives; external hard drives; and all external data storage devices such as disks, SANs, optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes), and non-volatile electronic media (e.g., flash drives), are covered under the provisions of this policy as follows:

1. University employees must safeguard institutional data by taking all due measures to secure this information.
2. IT@SAM maintains procedures for back-ups and redundancy to ensure the campus networked administrative data is protected in accordance with administrative directives.
3. All University personnel must practice safe measures for password protecting confidential information.
4. All university personnel must establish and follow procedures to ensure appropriate back-ups are made of any external or local storage devices maintained in their departments.
5. All university personnel must establish and abide with university policy and procedures to reduce risks associated with mobile devices.

6. University-owned computer and digital storage device must have all institutional data and licensed software reliably erased from the storage device and/or the storage device must be destroyed prior to its transfer of ownership using current best practices for the type of media.
7. When ownership of a computer or digital storage device is transferred, the device must be first transferred to IT@SAM for processing. This transfer includes both tagged asset and non-tagged asset equipment.
8. Any computer or digital storage device you wish to use for trade-in must be coordinated with IT@SAM for processing.
9. The University must have a confidentiality agreement in place with any vendor receiving devices that must be replaced as part of a warranty or repair contract but which cannot be erased for technical reasons.

**Related Policies, References and Attachments:**

An index of approved IT@SAM policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, May 15, 2011

Approved by: President's Cabinet, June 27, 2011

Next Review: November 1, 2014