

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

**Data Backup Policy: IT-11**

**Introduction:**

This policy requires SHSU information technology systems to have an effective backup of critical data under its management and for data owners, data custodians, system administrators and data users to use those processes. The processes should be based on the sensitivity, volatility, and value of the data as well as the difficulty of reproducing the data if and/or when needed.

The subject data for this policy, including determining which data and information is deemed 'critical' (i.e. confidential data and other data considered to be of institutional value) will be determined by the designated IRM.

**Scope:**

The SHSU Data Backup policy applies to any data owner, data custodian, system administrator and IT@SAM staff that installs, operates or maintains SHSU information technology resources.

**Policy Statement:**

1. Critical data as determined by the designated IRM must be backed up.
2. Archived backup data must be stored at a location that is physically different from its original creation and usage location.
3. The ability to retrieve and restore backup data must produce successful results. Verification, through restoration of backed-up data, must be performed on a regular basis as defined by the IT@SAM back-up procedures document for the respective system.
4. Procedures for backing up of critical data and the testing of the procedures must be documented. Such procedures must include at a minimum for each type of data:
  - a. A definition of the specific data to be backed up;
  - b. The type(s) of backup to be used (full backup, incremental backup, or a combination of both based upon a fixed schedule or trigger even such as scheduled maintenance);
  - c. The frequency and time of data backup;
  - d. The number of generations of backed up data that are to be maintained (both on site and off site);
  - e. Responsible individual(s) for data backup;
  - f. The storage site(s) for the backups;
  - g. The storage media to be used;
  - h. The naming convention for the labels on storage media;
  - i. Any requirements concerning the data backup archives (retention policies should be based on state and federal policies);
  - j. Transport modes; and

- k. Recovery of backed up data.
5. Each data backup process must have at least one primary and one secondary person in charge of the process who is committed to adherence to the specific data backup process established.
6. All departments should store data on network storage (e.g. S and T drives) rather than local storage (e.g. PC or Mac hard drive). Local storage is not backed up by IT@SAM.
7. IT@SAM administrators are responsible for backing up IT@SAM-managed servers and are required to implement a tested and auditable process to facilitate recovery from power or hardware failure, data and/or network problems, and physical disaster.
8. Requirements concerning the data backup archive:
  - a. Due to the concentration of data on backup data media, the degree of confidentiality and integrity of the backed up data must be at least as high as that of the original data. Consequently, appropriate security measures (e.g. access control, etc.) are required for data media.
  - b. Where records retention and disposition schedules need to be maintained, the data backup archive must be organized appropriately and equipped with the required erasure devices and procedures where technically feasible.
  - c. Any disks, tapes or other media used for backups must be disposed of in a manner consistent with IT@SAM IT-10.
9. Transport Modes: Data are transferred during any backup process. The following must be observed in such situations, irrespective of whether data are being transferred through a network, or whether data media are being dispatched to an archive. End-to-end security of the transmission path must be ensured for confidential data.
10. Recovery of Backup Data: Backup documentation including identification of critical data, programs, documentation and support items necessary to perform essential tasks during a recovery process must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.
  - a. Documentation of the restoration process must include procedures for the recovery from single-system or application failures or loss as well as a total center or department disaster scenario. Such procedures must include at a minimum for each type of data:
    - i. A definition of the specific data to be restored;
    - ii. The type(s) of backup to be used for restoral (full backup, incremental backup, or a combination of both based upon a fixed schedule or trigger even such as scheduled maintenance);
    - iii. The date and time of data backup to be restored;
    - iv. Individual(s) responsible for restoring data;
    - v. Individual(s) responsible for verifying restoral;
    - vi. Individual(s) needing access to recovered data and permission level needed;
    - vii. The storage site(s) for the backups to which the backups are restored;
    - viii. The storage media (e.g. tape, disk) to be used for restoral;

- ix. Any requirements concerning recovery;
- b. Recovery procedures must be tested and the tests documented on a periodic basis, but no less than annually. Testing ensures that the data can be recovered and that staff are familiar with the procedures.

**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, 2013