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

Data Backup and Recovery Policy: IT-11

PURPOSE:

The purpose of the Data Backup Policy is to manage and secure backup and restoration processes and the media employed within these processes; prevent the loss of data in the case of administrator error or corruption of data, system failure, or disaster; and ensure periodic restoration of data to confirm it is recoverable in a useable form.

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. IT@Sam System Administrators are responsible for backing up IT@Sam-managed servers and are required to implement a tested and auditable process to facilitate recovery from data loss.
2. 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 and will be the responsibility of the data owner.
3. SHSU IT@Sam System Administrators will perform daily data backups of all IT@Sam managed servers containing critical data for the purposes listed above.
    a. Individual drives (e.g. S drive) and email will be retained for 14 days.
    b. All other data, such as Enterprise Application Data (e.g. Banner and Oracle data) and shared storage backups (e.g. T drive) will be retained for 60 days.
    c. Policy exceptions to the stated retention times will be at the discretion of the President utilizing the IT@Sam Policy Exception Form .
    d. SHSU will not be responsible for data stored on non-SHSU cloud storage systems (e.g. One Drive) and data will be subject to that vendors' retention terms of service.
4. Determining which data and information is deemed 'critical' (e.g. confidential data and other data considered to be of institutional value) is the responsibility of the Data Owner, per SHSU Data Classification Policy (IT-06). Data identified by the Data Owner as non-critical may be excluded from this policy. Alternative backup schedules and media management may be requested by the data owner commensurate with the criticality of the data and the capabilities of the tools used for data storage.

5. Records retention is the responsibility of the Data Owner. The IT@Sam backups are not to be used to satisfy the retention of records and are not customized for all the varying retention periods.
6. Monthly backup data will be stored at a location that is physically different from the original data source.
7. 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.
8. 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 backup method to be used (full backup, incremental backup, differential, mirror, or a combination).
    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. The 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.
    j. The data transport modes.
        i. For data transferred during any backup process, end-to-end security of the transmission path must be ensured for confidential data.
    k. The recovery of backed up data.
        i. Processes must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.
    l. The destruction of obsolete backup media as described in SHSU Media Sanitization Policy (IT-15).

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, VP for Information Technology, June 28, 2016
Approved by: President's Cabinet, March 6, 2013
Next Review: November 1, 2018