College of Osteopathic Medicine
SAM HOUSTON STATE UNIVERSITY

Element 9.4: Secure Student Recordkeeping

- **9.4-1 Supporting Documentation**
  - Policies and Procedures on Student Recordkeeping – link

Policies and Procedures for Secure Student Record Keeping

Sam Houston State University (SHSU) has an accurate, confidential and secure system for secure student record keeping. The SHSU Records Retention Policy complies with all Federal and State guidelines regarding record retention as documented in the SHSU Records Retention Policy which may be accessed at: http://library.shsu.edu/about/RecordsRetention.pdf.

Documents not specifically listed in the above policy have the following retention policy:

- SHSU-COM meeting minutes – 7 years from date of meeting
- SHSU-COM sign-in sheets – 7 years from date of sign-in sheet
- SHSU-COM student records including, but not limited to: advising, academic and career counseling, evaluation, and grading data – 7 years from graduation or departure from the program
- Admissions Data stored in AMP – 7 years from application date

SHSU has established an Information Security Program that provides direction for managing and protecting the confidentiality, integrity, and availability of SHSU information technology resources. The program contains administrative, technical, and physical safeguards to protect student and University privileged information. The program defines the roles and responsibilities related to information security, including that of a full-time Information Security Officer (ISO) to oversee the program's various components.

The Information Technology Data Backup and Recovery Policy (IT-11) outlines steps for the protection of information technology data assets. Electronic data is stored on physically and electronically secured servers. Daily backup procedures are in place. Backup tapes are stored in a vault in a building separate from the servers. Academic records that predate electronic storage are retained in a vault and/or in locations with double locks.

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

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 Sam Houston State University (SHSU) Data Backup policy applies to any Information Owner, Information Custodian, system administrator and information Technology staff that installs, operates, or maintains SHSU information technology resources.

POLICY STATEMENT:

1. Information Technology 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., T drive, OneDrive) rather than local storage (e.g., Windows or Mac hard drive). Local storage is not backed up by IT@Sam and will be the responsibility of the Information Owner to protect the data with adequate backups.

3. Information Technology will perform daily data backups of all Information Technology managed servers containing critical data for the purposes listed above.

   a. Individual drives (e.g., S drive, profile) 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, Files) will be retained for 60 days.
   c. Policy exceptions to the stated retention times will be at the discretion of the President utilizing the Information Technology Policy Exception Form .
   d. SHSU will not be responsible for data stored on non-SHSU storage systems and data will be subject to those vendors' retention terms of service.

4. Data identified by the Information Owner as non-critical may be excluded from this policy.

5. Alternative backup schedules and media management may be requested by the Information Owner commensurate with the criticality of the data and the capabilities of the tools used for data storage.

6. Records retention is the responsibility of the Information Owner. The Information Technology backups are not to be used to satisfy the retention of records and are not customized for all the varying retention periods.

7. Backup data will be stored at a location that is physically different from the original data

source.

8. Verification, through restoration of backed-up data, must be performed on a regular basis as defined by the Information Technology back-up procedures document for the respective system.

9. 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).

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, April 17, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, April, 2023
Next Review: April, 2024