TEXAS SOUTHERN UNIVERSITY

MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **NUMBER: 04.06.28**
AREA: Computer and Information Technology

TITLE/SUBJECT: Personally Identifiable Information Policy

I. POLICY STATEMENT

Texas Southern University ("TSU") collects Personally Identifiable Information ("PII") for various reasons. PII is data which can be used to distinguish or determine an individual's identity, such as name or social security number, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date of birth, place of birth or mother's maiden name, etc. Examples of PII range from an individual's name or email address to an individual's financial and medical records and/or criminal history. Unauthorized access, use, or disclosure of PII can seriously harm individuals, by enabling the opportunity for identity theft, blackmail, or embarrassment. The disclosure of PII can also cause TSU to suffer a reduction in public trust and can create a legal liability.

Personally Identifiable Information that is captured and maintained at Texas Southern University should be considered protected data and thorough research needs to be done, before this data is altered by any individual employed by the institution or who contracts with the institution. It is important to maintain the integrity of the data and information stored in TSU systems or passed back and forth through third-party systems.

This policy covers students, applicants for admission, employees, applicants for employment, donors, alumni, research subjects, and others on whom TSU may have such information. The policy applies to all persons exposed to PII, its storage mechanisms (how the information is stored - e.g. paper, electronic, other media) and modes of transmission.

II. PURPOSE AND SCOPE

The purpose of this policy is to ensure: (a) that employees understand the need to safeguard this information, and (b) that adequate procedures are in place to minimize this risk of improper disclosure of PII. Access to PII information may only be granted to authorize individuals on a need to know basis.

This policy seeks to ensure the security, confidentiality and appropriate use of all personally identifiable information processed, stored, maintained, or transmitted on TSU computer systems and networks. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

1. Texas Southern University supports the protection of individual privacy. It recognizes the numerous and complex laws that govern the collection, storage, transfer, use and access to personally identifiable information. The University shall comply with all applicable laws that govern the collection, storage, transfer, use of, and access to personally identifiable information.

   TSU shall strive to minimize the collection of personally identifiable information, regardless of its source or medium to the least amount of information required to complete a particular transaction or to fulfill a particular purpose related to the academic or business needs of the institution. University administrators, faculty, staff and other representatives should limit any request for personally identifiable information to the minimum necessary or appropriate to accomplish the university-related purpose for which it is requested.

2. All Personally Identifiable Information in the possession of Texas Southern University is considered confidential unless:

   2.1. The data owner has authorized the release of information designated as "Directory Information" by the University; or

   2.2. The data owner has otherwise authorized its disclosure.

3. TSU requires that the following pieces of PII may not be collected, stored or used except in situations where there is legitimate business need and no reasonable alternative:

   3.1. Social Security Number

   3.2. Date of birth

   3.3. Place of birth

   3.4. Student/Employee ID number

   3.5. Mother's maiden name

   3.6. Credit card numbers

   3.7. Bank account numbers

   3.8. Income tax records

   3.9. Driver's license or other government-issued identification numbers

4. Consistent with applicable law and University policy, custodians of PII shall take reasonable and appropriate steps to:

    4.1. limit access to and further use or transfer of such information

    4.2. ensure that the information is maintained in a form and manner that is appropriately secure in light of the nature and sensitivity of the information

5. How to Protect Personally Identifiable Information:

    5.1. Electronic Storage and Disposal

        5.1.1. Do not store PII on a PDA, laptop computer or desktop computer's hard drive, USB drive, CD, flash memory card, floppy drive or other storage media.

        5.1.2. Do not store PII in public files accessible via the Internet.

        5.1.3. Do not download PII from TSU Banner databases unless legally required or for a standard TSU business practice.

        5.1.4. Do not transmit PII to external parties via email or the Internet unless the connection is secure or the information encrypted.

        5.1.5. Do not transmit PII via PDA, laptop, tablet or any other wireless technology.

        5.1.6. Discard media (such as disks, tapes, hard drives) that contain PII in a manner that protects the confidentiality of the information. Contact OIT to confirm disposal process.

    5.2. Physical Storage and Disposal

        5.2.1. Do not publicly display PII or leave PII unattended, even on your desk or on the desk of a co-worker.

        5.2.2. Do not take PII home.

        5.2.3. Do not discard PII in the trash. Shred PII when it is no longer needed.

    5.3. Security

        5.3.1. Lock your computer when unattended.

        5.3.2. Lock offices, desks, and files that contain PII when unattended.

        5.3.3. Eliminate the use of forms that ask for PII whenever possible.

5.3.4. Password-protect all accounts with access to PII.

5.3.5. Do not share passwords and do not document passwords.

5.4. Legal Disclosure Requirements

5.4.1. Do not share PII documents or information with anyone unless required by government regulations, specific TSU job responsibilities or business requirements. Be prepared to say "no" when asked to provide that type of information.

5.4.2. Do not communicate confidential student information designated by the Family Educational Rights and Privacy Act ("FERPA").

5.4.3. Notify TSU Information Security Officer or the Office of Information Technology Chief Information Officer (CIO) immediately if you suspect PII may have been compromised.

6. Laws and Regulations relating to Personally Identifiable Information

6.1. FERPA—Family Educational Rights and Privacy Act. Limits the disclosure of "education records" defined as those records that are: (a) "directly related" to a student, and, (b) maintained by or on behalf of the university.

6.1.1. A record is "directly related" to a student if it is "personally identifiable" to the student.

6.1.2. A record is "personally identifiable" to a student if it expressly identifies the student by name, address, birth date, social security number, ID number, or other such common identifier.

6.1.3. Examples of "education records" at TSU include registrar records, transcripts, papers, exams, individual class schedules, financial aid records, financial account records, disability accommodation records, disciplinary records, placement records.

6.2. HIPAA—Health Insurance Portability and Accountability Act. Imposes privacy and security standards addressing the use, disclosure, storage and transfer of "protected health information".

6.2.1. "Protected health information (PHI)" means "individually identifiable health information," which is any information that identifies an individual and relates to the individual's: past, present or future physical or mental health or condition.

6.2.2. Examples of information that should be treated as "protected health information" at TSU include employee benefit plan information, worker's compensation claim information, student health services information and student counseling center information.

6.3. GLB—Gramm-Leach-Bliley Act. Requires implementation of a written information security program for "customer information."

6.3.1. "Customer information" means any record containing "nonpublic personal information" handled or maintained by or on behalf of the institution about a customer of that institution.

6.3.2. Examples of "customer information" at TSU include financial records of employees (such as loans), students and their parents (such as cashier's accounts or information related to financial aid), and donors.

6.4. PCI-DSS –Payment Card Industry Data Security Standards. Requires implementation of security standards surrounding the authorization, processing, storage, and transmission of credit card data. The security standards apply to electronic and paper credit card data.

6.4.1. "Credit card data," as defined by PCI-DSS, is the first six and/or the last four digits of any credit card provided by a customer to conduct University business. If all digits of the credit card are used in the conduct of University business, then name, card expiration date, and source code are considered "credit card data"; and, hence, must be protected.

6.5. Texas Identity Theft Enforcement and Protection Act. Requires implementation and maintenance of reasonable procedures to protect information collected or maintained in the regular course of business from unlawful use or disclosure, including personal identifying information and sensitive personal information.

7. Disciplinary Action

Violation of this policy may result in disciplinary action, up to and including termination of employment pursuant to the University's Discipline & Termination Policy (staff) and Faculty Manual (faculty).

8. Applicable TSU Security Policy Standards

Security Standard 1, Security Standard 2, Security Standard 3, Security Standard 4, Security Standard 5, Security Standard 6, Security Standard 7, Security Standard 15, Security Standard 16, Security Standard 17

9. Review and Responsibilities

Responsible Party: Chief Information Officer

Review: Every 3 years, on or before September 1st

Forms

None

V. APPROVALS

Chief Information Officer

President

Effective Date 2/1/2018