Policy on Personally Identifiable Information (PII)	
Responsible Official: Chief Information Officer	**Responsible Office**: Information Technology Services

Policy Purpose

East Tennessee State University (ETSU) creates, collects, maintains, uses, and transmits Personally Identifiable Information (PII) relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. ETSU is committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations to maximize trust and integrity.

This policy applies to all members of the ETSU community, including all full-time and part-time employees, faculty, students and their parents or guardians, and other individuals such as volunteers, contractors, consultants, other agents of the community, alumni and affiliates that are associated with the University or whose work gives them custodial responsibilities for PII.

Policy Statement

Members of the ETSU community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it. All individuals who dispense, receive, and store PII have the responsibility to safeguard that information.

In adopting this policy, the University is guided by the following objectives:

1. To enhance individual privacy for members of the ETSU community through the secure handling of PII.
2. To ensure all members of the ETSU community understand their obligations and individual responsibilities under this policy by providing appropriate training that shall permit the ETSU community to comply with both the letter and spirit of all applicable privacy legislation.
3. To increase the security and management of Social Security Numbers (SSNs) by:
    a. Instilling broad awareness of the confidential nature of SSNs;
    b. Establishing a consistency with regard to the use of SSNs throughout the University;

c. Complying with all Payment Card Industry (PCI) standards
d. Complying with any other applicable and required standards, regulations and/or laws; and
e. Complying with the Family Educational Rights and Privacy Act of 1974 (FERPA).

4. Appoint data custodians who are responsible for oversight of personally identifiable information in their respective areas of institutional operations. Activities of these officials are aligned and integrated through appropriate coordination among institutional officials.

I. Policy Requirements

Officials responsible for each of the following areas shall be considered data custodians:

a. Student Records
b. Financial Aid Records
c. Alumni and Donor Records
d. Employee Records
e. Purchasing and Contracts
f. Research Subjects
g. Public Safety or Campus Police

II. Management and Distribution of Personally Identifiable Information

a. PII may be released only on a minimum necessary basis and only to those individuals who are authorized to use such information as part of their official ETSU duties, subject to the following requirements:
    i. That the PII released is narrowly tailored to a specific busines requirement;
    ii. That the information is kept secure and used only for the specific official University purposes for which authorization was obtained; and
    iii. That the PII is not further disclosed or provided to others without proper authorization as defined above.
b. PII may be handled by third parties, including cloud service providers, with the strict requirement that the information be kept secure and used only for a specific official authorized business purpose as defined in a Business Associate Agreement with that third party. Third party vendors must meet the information security qualifications established in the Higher Education Community Vendor Assessment Tool (HECVAT) prior to PII transfer to the third party.
c. Exceptions to the policy may be made only upon specific requests approved by the institutional official responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and business needs of the institution.
    i. Exceptions made must be documented, retained securely, and reviewed periodically by the appropriate institutional official or designee.
    ii. Exceptions may be modified or eliminated based on this review and shall be documented and retained for audit purposes.
d. Based on FERPA guidelines, directory information is information that is generally not considered harmful or an invasion of privacy if released and can be disclosed without

consent.

e. The University will notify students annually of their rights under FERPA.
f. Information that conforms to the HIPAA standards of de-identification or anonymization is not PII.

III. Management and Distribution of Government Issued Personal Identifiers

a. Social Security Number
    i. ETSU collects SSNs when:
        1. Required to do so by law;
        2. No other identifier serves the business purpose; and
        3. An individual volunteers the SSN as a means of locating or confirming personal records.
    ii. In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.
    iii. ETSU will release SSNs to persons or entities outside the institution only:
        1. As required by law;
        2. When permission is granted by the individual;
        3. When the external entity is acting as the institution's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to thirds parties; or
        4. When the appropriate Legal Counsel has approved the release.
    iv. SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a University official for a University business purpose.
    v. The release or posting of personal information, such as grades or occupational listings keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access.
    vi. SSNs will be transmitted electronically only for business purposes approved by the institutional officials responsible for SSN oversight and only through secure mechanisms.
    vii. The Data Custodians who are responsible for SSNs will oversee the establishment of business rules for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.
b. Non-SSN Government-Issued Identifiers
    i. During business operations, ETSU has access to collect and use non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers, Employee Identification Numbers, and military identification cards, among others.
    ii. ETSU shall follow the minimum necessary standard and safeguard these identifiers.

IV. Management and Distribution of Institution Issued Identifiers

a. The Institutional ID is a unique alphanumeric identifier assigned by the institution to any entity that requires an identifying number in an institutional system or record.
b. An Institutional ID is assigned at the earliest possible point of contact between the entity and the institution.
c. The Institutional ID is associated permanently and uniquely with the entity to which it is assigned.
d. The Institutional ID is considered PII by the institution, to be used only for appropriate business purposes in support of operations.
e. The Institutional ID is used to identify, track, and serve individuals across all institutional electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the institution and presence in the institution's systems or records.
f. The Institutional ID is not to be disclosed or displayed publicly by the Institution, nor to be posted on the Institution's electronic information or data systems unless the Institutional ID is protected by access controls that limit access to properly authorized individuals.
g. The release or posting of personal information keyed by the Institutional ID, such as grades, is prohibited.
h. Any document, item, file, or database that contains Institutional IDs in print or electronic form is to be protected and disposed of in a secure manner in compliance with data retention rules.

V. Responsibility for Maintenance and Access Control

a. Institutional IDs are maintained and administered by the appropriate institutional office in accordance with this policy. Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for use in accordance with this policy.
b. Access to electronic and physical repositories containing PII shall be controlled based on reasonable and appropriate administrative, physical, technical, and organizational safeguards.
c. Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority.
d. All paper documents with PII must be under lock and key or otherwise securely stored.
e. Document retention policies dictate schedules for PII deletion and/or destruction. Proper disposal of PII shall involve shredders (for paper), securely wiping/deleting data (for digital information) and other information security approved methods of eliminating this data.

VI. Enforcement

Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of personal identification numbers may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the institution or, in the case of students, suspension or expulsion from the

institution.

Authority: T.C.A § 49-8-203 et. Seq., Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. § 160 and 164; 45 C.F.R. § 164.302 - § 164.318., Federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), Open Records Act of Tennessee, Gramm Leach Bliley Act (Financial Services Modernization Act of 1999), Pub.L. 104–102 or 113 Stat. 1338. 15 U.S.C. § 6801-09; 16 C.F.R. § 313-314; T.C.A. § 47-18-2107.

Previous Policy: TBR Policy Personally Identifiable Information (PII): 1.08.04.00

Defined Terms

Data Custodians:	Data Custodians are individuals responsible for oversight of personally identifiable information in their respective areas of institutional operations.
Data Owner:	Also called a Data Steward, is the individual who has administrative control and has been officially designated as accountable for a specific information asset or dataset. This person determines who has access to what data and ITS implements the data controls as instructed.
Directory Information:	Directory information is generally not considered harmful or an invasion of privacy if released. It can also be disclosed to outside organizations. ETSU may release directory information including student names, addresses (e-mail, mailing, and campus box), major, and phone number. In addition, ETSU may also release other directory information. Other directory information is defined as: enrollment status, dates of attendance, classification, previous institution(s) attended, awards, honors (includes Deans List), degrees conferred (including dates), and sports participation information.
Minimum Necessary:	The standard that defines the least information and fewest people should be involved to satisfactorily perform a particular function.
Personally Identifiable Information (PII):	Information which can be used to distinguish or trace an individual's identity, such as their ID, Social Security Number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Policy History

Procedure

Procedure History

Effective Date:

Revision Date: February 11, 2022

Related Form(s)

Scope and Applicability

Primary: ETSU Employees and Students

Secondary: