Austin Peay State University

Personally Identifiable Information (PII)

POLICIES

Issued: March 25, 2017
Responsible Official: Vice President for Finance and Administration
Responsible Office: Information Technology

Policy Statement

Austin Peay State University is committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations in order to maximize trust and integrity.

Purpose

Austin Peay State University creates, collects, maintains, uses, and transmits personally identifiable information relating to individuals associated with the university including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. The university is committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations in order to maximize trust and integrity.

Contents

-Responsibility for Maintenance and Access Control
-Enforcement

Links
-Theft or Loss of Data

	Definitions
Data Custodians	Data Custodians are university designees who have planning and policy-making responsibilities for university data and the university Data Warehouse. The Data Custodians, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability.
Minimum Necessary	Minimum Necessary is the standard that defines that 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 name, 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.
Directory Information	Directory Information is determined by the university and is not considered PII.

	Procedures
Policy	A. Members of the university 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. B. All individuals who dispense, receive, and store PII have responsibilities to safeguard it. C. In adopting this policy, the university is guided by the following objectives:

1. To enhance individual privacy for members of the university community through the secure handling of PII and personal identifiers (PIDs);
2. To ensure that all members of the university community understand their obligations and individual responsibilities under this policy by providing appropriate training that will permit the university community to comply with both the letter and the spirit of all applicable privacy legislation.
3. To increase security and management of Social Security numbers (SSNs) by:
   a. Instilling broad awareness of the confidential nature of the SSNs;
   b. Establishing a consistent policy about the use of SSNs throughout the university; and
   c. Ensuring that access to SSNs for the purpose of conducting university business is granted only to the extent necessary to accomplish a given task or purpose.
   d. To reduce reliance on the SSN for identification purposes as much as possible.
4. To comply with all Payment Card Industry (PCI) standards
5. To comply with HIPPA standards (if applicable)

D. Data Custodians are responsible for oversight of personally identifiable information in their respective areas of university operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant university officials.

Scope

This policy applies to all members of the university community, including all full- and part-time employees, faculty, students and their parents or guardians, and other individuals such as 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 Requirements

A. Data Trustees
   1. Officials responsible for each of the following areas will be considered data custodians:
      a. Student Records
      b. Alumni and Donor Records
      c. Health Records
      d. Faculty and Staff Records
      e. Purchasing and Contracts

f. Research Subjects
g. Public Safety

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 university duties, subject to the requirements:
   1. That the PII released is narrowly tailored to a specific business requirement;
   2. That the information is kept secure and used only for the specific official university purposes for which authorization was obtained; and
   3. 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 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.

C. Exceptions to this policy may be made only upon specific requests approved by the cognizant university 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 university.
   1. Any and all exceptions made must be documented, retained securely, and reviewed periodically by the appropriate cognizant university official or his/her designee.

D. Directory Information, as defined by Federal and State law and university policy, will be published following the guidelines defined by the university.

E. Information that has been collected that conforms to the HIPAA standards of de-identification or anonymization is not PII.

Government-Issued Personal Identifiers

A. Social Security Number
   1. Provision of Information
      a. The university collects SSNs:
         1. When required to do so by law;
         2. When no other identifier serves the business purpose; and

3. When an individual volunteers the SSN as a means of locating or confirming personal records.

b. 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.

2. Release of SSNs
   a. SNs will be released to persons or entities outside the university only:
      1. As required by law;
      2. When permission is granted by the individual;
      3. When the external entity is acting as the university'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 third parties; or
      4. When the appropriate Counsel has approved the release.
3. Use, Display, Storage, Retention, and Disposal
   a. SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a cognizant university official for a university business purpose.
   b. 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.
   c. SSNs will be transmitted electronically only for business purposes approved by the university officials responsible for SSN oversight and only through secure mechanisms.
   d. 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
   1. In the course of its business operations, the university will have access to, collect, and use non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers,

Employee Identification Numbers (EIN), and military identification cards, among others.
2. The university shall follow the Minimum Necessary standard and strive to safeguard these identifiers.

University Issued Identifiers

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

Other Externally-Assigned Identifiers and Other Personally Identifiable Information

The university shall follow the Minimum Necessary standard and strive to safeguard any externally assigned identifiers which may be collected.

Responsibility for Maintenance and Access Control

A. University IDs are maintained and administered by the appropriate university office in accordance with this policy.
   1. Other university offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.

B. Access to electronic and physical repositories containing PII will be controlled based upon 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.

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 university or, in the case of students, suspension or expulsion from the university.

Links

Theft or Loss of Data http://www.apsu.edu/information-technology/theft-or-loss-data

Revision Dates

APSU Policy 4:040 – Issued: March 25, 2017

Subject Areas:

Academic	Finance	General	Human Resources	Information Technology	Student Affairs
				☑	

Approved

President: signature on file