**Austin Peay State University**

# Information Security and Data Classification Policy

**POLICIES**

**Issued:** August 17, 2018
**Responsible Official:** Vice President for Finance and Administration
**Responsible Office:** Office of Information Technology

## Policy Statement

It is the policy of Austin Peay State University to provide a security framework that will ensure the protection of university information from unauthorized access, loss, or damage. The university is committed to protecting all restricted and private data collected and maintained on university students, employees, donors, vendors and others.  This policy governs the use, control, and access to restricted data defined by statute, regulation, contract, license, or definitions within this policy. This policy also defines and governs the use of private and public university data. Included within this policy is the university data classification description and definition.

## Purpose

Austin Peay State University is committed to maintaining the confidentiality, integrity, and availability of all restricted, private, and public university data.  The purpose of this policy is to establish classifications for university data and a framework to preserve the integrity of all university information regardless of the medium, to include physical and electronic forms.

## Contents (if applicable)

-Integrity
-Payment Card Industry Security Standards (PCI-DSS)
-Personally Identifiable Information (PII)
-Protected Health Information (PHI)
-Virtual Private Network (VPN)

**Procedures**
-Who Is Affected By This Policy
-Data Classification
-Data Security
-Responsibilities
-Failure to Comply with this Policy

**Links**
-APSU Policy 1:016
-APSU Policy 4:029
-APSU Policy 4:031
-APSU Policy 4:040
-APSU Policy 4:041
-Access Control Guideline

## Definitions

**Availability**

Ensuring that data and services are available when needed.

**Confidentiality**

The assurance of data privacy and protection from unauthorized disclosure.

**Data vs. Information**

Data is raw, unorganized facts that are not meaningful until processed, organized, structured, or presented in a context that makes them useful. This context is called information.

**Encryption**

Programs and measures to encode data such that it cannot be decoded and read without knowing an appropriate secret key.

**Enterprise Information System (EIS)**

Any centralized data storage or distribution system on the university network. Enterprise information systems are managed by the Information Technology department.

**Family Educational Rights and Privacy Act (FERPA)**

Federal legislation that protects the privacy of students' personally identifiable information (PII) and governs its access and disclosure. The act applies to all educational institutions that receive federal funds.

**Gramm-Leach-Bliley Act (GLBA)**

Federal law that defines and controls how financial institutions handle, secure, and destroy customers’ private information.

**Health Insurance Portability and Accountability Act (HIPAA)**

Federal law designed to provide privacy standards to protect patient’s medical records and other health information provided to health plans, doctors, hospitals, and other health organizations.

**Integrity**

The protection of data from unauthorized modification, both malicious and accidental.

**Payment Card Industry Data Security Standards (PCI-DSS)**

Proprietary standard for organizations that handle branded credit cards mandated by the major credit card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls for cardholder data to reduce credit card fraud.

**Personally Identifiable Information (PII)**

Any information about an individual maintained by the university, including any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

**Protected Health Information (PHI)**

Any information created, received, maintained, processed or transmitted by the university that relates to the past, present, or future physical or mental health of an individual, the provision of health care to an individual, or the past, present or future payment for health care, and identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

**Virtual Private Network (VPN)**

The extension of a private network across a public network, enabling users to send and receive data across the public network as if their computers or devices were directly connected to the private network. The VPN creates a secure, encrypted tunnel between the end user and the private network.

## Procedures

**Who Is Affected By This Policy**

This policy applies to all university faculty and staff, as well as students acting on behalf of Austin Peay State University including, but not limited to, student workers, student interns, and graduate assistants. This policy also applies to all other individuals and entities granted use of university data and information including, but not limited to, contractors, vendors, temporary employees, and volunteers.

## Data Classification

Austin Peay State University has adopted the following three classifications of university data:

A. **Restricted Data**: Any information protected by federal, state, or local laws and regulations or industry standards; to include HIPAA, GLBA, FERPA, and PCI-DSS. Restricted Data includes but is not limited to PII and PHI information, Social Security numbers, credit card numbers, bank account numbers, and driver’s license numbers.

B. **Private Data**: Any information that is proprietary or produced only for use by members of the Austin Peay State University community who have a legitimate purpose to access such data. Private Data includes but is not limited to internal operating procedures and operational manuals. Internal memoranda, emails, reports and other documents, and technical documents such as system configurations and floor plans.

C. **Public Data** – Any information that can be made available to the general public with no legal restrictions on its access or use. Public Data includes but is not limited to general access data on the university websites, campus maps, directory information (except for students who explicitly request to restrict their directory data), and university financial statements and reports generally available to the public.

## Data Security

### A. General Security

All university personnel and agents of the university with access to restricted and/or private data must ensure that this data is protected against physical theft or loss, electronic invasion, or unintentional exposure. All university personnel and agents of the university must also protect all university data against loss of integrity.

### B. Electronic Security

#### I. General Security

Electronic Restricted data must only be stored on university owned and protected Enterprise Information Systems (EISs), the university file server system, and cloud applications that have a contractual relationship with the university and have adequately addressed compliance with university data security, privacy, and IT management requirements. The Information Technology department is responsible for the management and security of all EISs.

Electronic Private data may be stored on university owned desktops and laptops that are protected with university required encryption and security applications, and where all operating system patches and updates are applied as scheduled by the Information Technology department. Private data may also be stored on university authorized cloud applications and cloud storage solutions. Private data may not be stored on personally owned computers or devices.

### II. Remote Access

Remote access to restricted and private data is available only to authorized personnel and agents of the university. Personnel must be authenticated to access restricted and private data, the data must be encrypted during transit, and the remote access must be via university supported VPN.

### III. Portable Devices and Media

Restricted data may not be stored on any portable device and media.

Private data may be stored on university supplied portable devices and media that have adequate protective measures implemented to safeguard the confidentiality and integrity in the event of theft or loss. Users in possession of private data on portable devices and media are responsible for protecting the data.

### IV. Equipment Disposal

University owned computers, portable devices, and portable media must have all university data permanently erased before transferring out of university control, and/or destroyed, by the Information Technology department.

**Responsibilities**

All Austin Peay State University faculty, staff, students acting on behalf of the university, and others granted use of university data and information are expected to:

1. Understand the data classification levels defined in this policy.
2. As appropriate, classify the data and information for which one is responsible accordingly.
3. Access university data and information only as needed to meet legitimate business needs.
4. Not divulge, copy, release, sell, loan, alter, or destroy any university data or information without a valid business purpose and/or authorization.
5. Protect the Confidentiality, Integrity, and Availability of university data and information in a manner consistent with the classification level and type.
6. Handle information in accordance with any other applicable university standard or policy.
7. Safeguard any physical key, ID card, computer account, or network account that allows one to access university data and information.
8. Discard media containing Austin Peay State University data and information in a manner consistent with the classification level, type, and any other applicable university retention requirement. This includes data and information contained in any hard copy document, or in any electronic, magnetic, or optical storage medium.
9. Contact the Office of the General Counsel prior to responding to any litigation or law enforcement subpoenas, court orders, open records requests, and other requests from private litigants and/or government agencies.
10. Contact the appropriate university office prior to responding to requests for information from regulatory agencies, inspectors, examiners and/or auditors.
11. All university units and departments are responsible for developing procedures for handling, disposing of, and securing Restricted and Private Data in physical form.

**Failure to Comply with this Policy**

Failure to comply with current Data Security procedures may result in limiting or denying access to university data resources. If, upon investigation by the appropriate university officials, the lack of compliance appears to have been willful and deliberate or if there is repeated lack of compliance, disciplinary action up to and including termination may be taken.

## Links

| | |
|---|---|
| **APSU Policy 1:016** | http://www.apsu.edu/policy/1s_governance_organization_and_general_policies/1016-preventing-and-reporting-fraud-waste-or-abuse.php |
| **APSU Policy 4:029** | http://www.apsu.edu/policy/4s_business_and_finance_policies/4029-acceptable-use-information-technology-resources.php |
| **APSU Policy 4:031** | http://www.apsu.edu/policy/4s_business_and_finance_policies/4031-identity-theft-prevention.php |
| **APSU Policy 4:040** | http://www.apsu.edu/policy/4s_business_and_finance_policies/4040-personally-identifiable-information.php |
| **APSU Policy 4:041** | http://www.apsu.edu/policy/4s_business_and_finance_policies/4041-safeguarding-nonpublic-financial-information.php |
| **Access Control Guideline** | https://www.apsu.edu/information-technology/infosec/policies/accesscontrolguideline.pdf |

## Revision Dates

APSU Policy 4:042 – Issued: August 17, 2018

## Subject Areas:

| Academic | Finance | General | Human Resources | Information Technology | Student Affairs |
|---|---|---|---|---|---|
| | | | | ☑ | |

## Approved

President: signature on file