Austin Peay State University
Identity Theft Operating Standards
(APSUITOS)

I. PROGRAM ADOPTION

Austin Peay State University establishes Identity Theft Operating Standards pursuant to the Federal Trade Commission's Red Flags Rule, which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). These Standards also encompass the rules and regulations set forth by the Gramm-Leach-Bliley Act (GLBA). These Standards incorporate the policies and procedures documented in Austin Peay State University policies: 4:031, 4:040, and 4:041.

APSU Policy **4:031 Identity Theft Prevention** can be accessed at:
http://www.apsu.edu/policy/4s_business_and_finance_policies/4031-identity-theft-prevention.php

APSU Policy **4:040 Personally Identifiable Information** can be accessed at:
http://www.apsu.edu/policy/4s_business_and_finance_policies/4040-personally-identifiable-information.php

APSU Policy **4:041 Safeguarding Nonpublic Financial Information** can be accessed at:
http://www.apsu.edu/policy/4s_business_and_finance_policies/4041-safeguarding-nonpublic-financial-information.php

In addition, Austin Peay State University establishes the following standards in regards to Red Flag detection, Identity Theft prevention and Program administration:

II. ADDITIONAL DEFINITIONS

A. Program Administrator

The Program Administrator is the individual responsible for the oversight of the program.

B. Service Provider

Service Provider is a person, business, or any other entity that provides a service to or for Austin Peay State University.

C. Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is a category of sensitive information that is associated with a specific person and that can be used to uniquely identify, contact, or locate a specific person either alone or when combined with other personal or

identifying information that is linked or linkable to that person. PII should be accessed only on a strictly need-to-know basis and handled and stored with care. Personal data that is maintained in a way that does not allow association with a specific person is not considered PII. PII does not include publicly available information that is lawfully made available from federal, state, or local governments.

III. GOVERNMENT REGULATIONS

A. Red Flag

The rules implementing section 114 require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. The Program must contain ‘‘reasonable policies and procedures’’ to: Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program; Detect Red Flags that have been incorporated into the Program; Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

B. GLBA

The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting financial institutions. The law requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information. The key rules under the GLBA that concern Austin Peay State University are:

1. *The Financial Privacy Rule* which governs the collection and disclosure of customers’ personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information.

2. *The Safeguards Rule* requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions.

IV. IDENTIFICATION OF RED FLAGS

In order to further identify relevant Red Flags, Faculty and Staff of Austin Peay State University will consider these additional Red Flags.

A. Suspicious Account Activity or Unusual Use of Account

- Unauthorized access to or use of PII.
- Excessive failed logon attempts.
- Frequent account lockouts due to failed logon attempts.

B. Missing or Stolen Identifying Information

- Missing or stolen computer systems.
- Missing or stolen removable storage media.
- Missing or stolen printed media containing PII.
- Buildings, rooms, offices, file cabinets, desk drawers, overhead cabinets, and any other storage space that appears to have been forcibly opened or accessed by unauthorized personal.
- Any suspected theft of documents containing PII.

IV. DETECTING RED FLAGS

A. New Accounts

In order to further detect Red Flags either identified within APSU policies or within this document that are associated with the opening of a new account, Austin Peay State University personnel will take the following steps to obtain and verify the identity of the person opening the account.

1. Review documentation showing the existence of a business entity or service provider.
2. Independently contact the person.
3. Compare information given with information from other sources.

V. MITIGATING IDENTITY THEFT

In the event Austin Peay State University personnel detect identified or suspected Red Flags, such personnel ***will*** take the following actions:

1. Monitor the covered account for evidence of Identity Theft.
2. Notify management for determination of the appropriate step(s) to take.
3. Notify the Program Administrator for determination of the appropriate step(s) to take.
4. Complete a Suspicious Activity Report (SAR) detailing the Red Flag, actions taken by Austin Peay State University, and the final outcome.

Depending upon the degree of risk posed by the Red Flag, Austin Peay State University ***will*** take one or more of the following actions:

1. Contact the person with the covered account.
2. Change any passwords or other security codes and devices that permit access to a covered account.

3. Close an existing covered account.
4. Reopen a covered account with a new number and password.
5. Remove access to all covered accounts.
6. Refrain from attempting to collect payment on a compromised covered account.
7. Alert students, faculty, and staff of covered account breach.
8. Contact the media.
9. Notify law enforcement.
10. Cancel the transaction.
11. Determine that no response is needed under the particular circumstances

VI. PREVENTING IDENTITY THEFT

In order to prevent Identity Theft from occurring, Austin Peay State University will take the following steps with respect to its internal operating procedures to protect identifying information. These steps are in addition to those established in **4:031 Identity Theft Prevention.**

A. Network/Computer Procedures – These procedures are to be completed by the Information Technology (IT) department of Austin Peay State University. However, it is the responsibility of all employees to ensure that their actions do not undermine the procedures set forth here.

1. Monitor the Austin Peay State University website for PII and remove it when detected.
2. Provide password protection for all computers.
3. Use pin numbers with the maximum digits allowed.
4. Encourage the use of **Strong Passwords,** where and when possible.
    a. Avoid the use of words from a dictionary in any language, including common or clever misspellings of words.
    b. Do not create a new password that simply increments a digit in your current password.
    c. Avoid the use of passwords that begin or end with a numeral because they can be guessed easier than passwords that have a numeral in the middle.
    d. Avoid the use of passwords that others can easily guess by looking at your desk (such as names of pets, sports teams, and family members).
    e. Avoid the use of words from popular culture. Enforce the use of passwords that require you to type with both hands on the keyboard.
    f. Enforce the use of uppercase and lowercase letter, numbers, and symbols in all passwords where applicable.
5. Enforce lockout procedures on all software to 10 or less failed logon attempts where possible.
6. Create security schemas to limit access to PII
7. Maintain a secure environment for backup media.
8. Maintain up to date firewalls.
9. Obtain, test, and install software patches promptly.
10. Monitor the security of the Austin Peay State University network.

11. Store electronic PII on secure servers.
12. Keep all servers that store PII in a physically secure area.
13. Use IPS/IDS tools to monitor and prevent intrusions to the network.
14. Create Security Baselines to describe all the steps required to configure a computer system, to provide security, and how to administer and maintain that level of security.
15. Create roles to restrict the access of PII to only those that have a business need to view such information.
16. Create roles to restrict the update privileges of PII to only those that have a business need to update such information.
17. Utilize encryption when transmitting PII.
18. Create a security group within Windows Server 20xx to set the following settings:
    a. Enforce Password History, set to 24
    b. Maximum Password Age, set to 120
    c. Minimum Password Age, set to 1
    d. Minimum Password Length, set to 8
    e. Password Must Meet Complexity Requirements, set Enabled
    f. Store Password Using Reversible Encryption, set Disabled
    g. Account Lockout Duration, set to 0
    h. Account Lockout Threshold, set to 10
    i. Reset Account Lockout Counter After, set to 0
19. Avoid storage of PII on machines that are publicly facing on the Internet.
20. Properly dispose of old or damaged electronic devices that are capable of storing PII.

B. Personnel Procedures – These procedures are to be completed by every employee of Austin Peay State University.

1. Lock computers when leaving unattended by pressing **Ctrl/Alt/Delete** and selecting Lock Computer.
2. Do not provide personal Username/Password information to anyone.
3. Do not leave Username/Password information in plain sight.
4. Keep only the kinds of PII necessary for the job at hand and secure this documentation when leaving your office to prevent unauthorized access.
5. Secure fax transmissions from unauthorized access.
6. Limit access to PII to only those who have a business need to see such information.
7. Do not give, sell, or trade PII.
8. Limit the removal of university owned portable computing devices and removable media from its premises and return them as soon as possible. Portable computing devices and removable media can include but are not limited to: laptop/notebook computers, PDA's, external hard drives, thumb/USB drives, CD's and DVD's, floppy discs.
9. Keep portable computing devices and removable media in your possession at all times when not on Austin Peay State University property. Locked in a home or hotel room **is** considered "in your possession". Locked in a car **is not** considered "in your possession".

10. Keep portable computing devices locked in an office, or secured with a cable lock to a stable structure, or in your possession when on Austin Peay State University property.
11. Use extreme caution when opening e-mails and attachments. These may contain viruses or other malicious code.
12. Refrain from taking PII home.
13. Refrain from emailing PII, even as an attachment.
14. Refrain from storing PII on removable media.
15. Refrain from storing PII on a laptop or desktop computer.
16. Refrain from using 3rd party software not authorized by IT to transmit files that contain PII.
17. Violations to this program are subject to the Discipline Procedures set forth in Austin Peay State University policy number 5:053.

C. Email Remediation—These steps are to be followed in the event an email containing PII is received from an email account external to Austin Peay State University.

1. If an unsolicited email, from an unsecure account (non-APSU email), containing PII is received, the following steps are followed:
    a. The university employee receiving the email will reply to the sender. The reply includes notification of the university's inability to accept information via unsecure means and options for secure submission or inquiries. Note that the reply must not contain the original PII information.
    b. The email and all its contents are to be permanently purged from the email program.

2. Emails are required to be encrypted in instances where university employees need to transmit PII information to individuals via unsecure email accounts. Passwords are sent in separate emails.

D. Authenticating Identity Procedures —These steps are to be followed in the event financial information is to be shared with a student.

1. <u>If In-Person:</u>

    The Individual must present:

    a. APSU Student ID; or
    b. Unexpired valid government photo ID
        - Driver's License
        - Non-Driver's Identification Card
        - Other State Issued ID
        - U.S. Passport
        - Department of Defense ID

2. If by Telephone
    c. A student must verify his or her name and date of birth. A prospective student without a student ID number need not verify this information since financial data is not loaded into our system until a student ID number exists.
    d. An individual permitted access to information via the FERPA Release Form must verify his or her designated pin number. If FERPA rules are not applicable due to a student being an incoming freshmen prior to the first day of courses, the parent must provide the student's name and date of birth. Additionally, the parent must provide his or her name and date of birth.

VII. PROGRAM UPDATES

The Program will be periodically reviewed and updated to reflect changes in risks to covered accounts and to the safety and soundness of Austin Peay from Identity Theft. The Program Administrator shall (at least annually) consider university experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the university maintains, and changes in university business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall initiate a revised Program and present the changes to the President of Austin Peay State University, and the Vice Presidents of Austin Peay State University for their review and approval.

VIII. Program Administration

The Program Administrator shall be responsible for developing, implementing and updating the Program.

A. Program Administrator responsibilities

1. The Program administration
2. Train Austin Peay Faculty/Staff on the Program
3. Review any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft
4. Determine which steps of prevention and mitigation should be taken in particular circumstances.
5. Inform faculty and staff of any recent or significant events via email or Austin Peay State University website.
6. Consider periodic changes to the Program.

B. Faculty/Staff Training

Austin Peay State University Faculty and Staff will receive Identity Theft training individually as part of their new hire process. Faculty and Staff will also receive annual training collectively. This training will be up-to-date with the current Program and will include any changes to the Program, as well as an analysis of Austin Peay State University experience with Identity theft from the previous year(s). This mandatory training will either be conducted as a group seminar or through the Austin Peay website as an online tutorial. All training materials will be available on the Austin Peay State University website.

C. Suspicious Activity Reports (SARs)

Austin Peay State University Faculty and Staff will complete an SAR after any Red Flag event. The SAR will be sent to the Program Administrator and will be copied to appropriate department heads. The SARs will be used to help determine the threats against Austin Peay, the response from Austin Peay, and the effectiveness of the response. Information from SARs will be used in an annual report concerning the effectiveness of the Red Flag program and will be used to further update the Program. SARs will contain the following information:

1. Details of Red flag event
2. Parties involved (victims, assailants, employees, etc.)
3. Actions taken by Austin Peay State University
4. Final outcome
5. Recommendations

D. Annual Red Flag Program Report

The annual Red Flag Program report will be prepared by the Program Administrator. It will be presented to the Austin Peay Administration for review and to Faculty/Staff during annual Red flag training. It will include:

1. An analysis of the effectiveness of the Red Flag Program.
2. The current risk of identity theft at Austin Peay State University.
3. A review of Red Flag incidents.
4. Highlights of significant incidents and Austin Peay State University response.
5. New and existing service provider agreements.
6. Recommendations for material changes to the Program.

IX. Oversight of Service Provider Arrangements

In the event Austin Peay State University engages a service provider to perform an activity in connection with one or more accounts, the university will take the following steps to ensure the service provider performs its activity in accordance with reasonable

policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place.
2. Require, by contract, that service providers review the Austin Peay State University Program and report any Red Flags to the Program Administrator.
3. Require, by contract, that any 3rd parties or subcontractors used by service providers have such policies and procedures in place and adhere to the Austin Peay State University Program.