Austin Peay State University

Safeguarding Nonpublic Financial Information

POLICIES

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

Policy Statement

It is the policy of Austin Peay State University Federal law requires that financial institutions, the University, comply with the Gramm-Leach-Bliley Act and, in so doing, safeguard the confidentiality of nonpublic financial information of its constituents. This Policy is issued to aid APSU in drafting Information Security Programs to comply with the Federal Trade Commission's "Standards for Safeguarding Customer Information" Rule promulgated under the authority of the Gramm-Leach-Bliley Act.

Purpose

This policy explains the procedure by which the University must develop a comprehensive written Information Security Program (the "Program") as mandated by the Gramm-Leach-Bliley Act ("GLBA") Standards for Safeguarding Customer Information Rule. The University's Program must include the components described below pursuant to which the institution intends to:

1. Protect the security and confidentiality of customers' nonpublic financial information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

The Program may consist of existing university policies and procedures that are incorporated by reference into the Program, including but not limited to policies such as, computer / electronic records confidentiality policies, Family Educational Rights &

Privacy Act policies, employee/personnel records confidentiality policies, etc.

Contents

Definitions

Customer	Defined as a consumer who has a customer relationship with a financial institution.
Consumer	An individual (or that individual's legal representative) who obtains or has obtained a financial product or service from a financial institution that is used primarily for personal, family, or household purposes.

Non-public financial information	Any record that an institution obtains from a customer in the process of offering a financial product or service, or such information provided to the institution by another financial institution. The term nonpublic financial information means any information:
	• That a student or other third party provides in order to obtain a financial service from the institution:
	  ○ About a student or other third party resulting from any transaction with the institution involving a financial service; or
	  ○ Otherwise obtained about a student or other third party in connection with providing a financial service to that person; and
	• Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is

	derived using any personally identifiable financial information that is not publicly available.
Offering a financial product or service	Includes, but is not limited to: • Offering/processing student loans; • Granting emergency or long term loans to students or employees; • Receiving income tax information from a student's parent when offering a financial aid package; • Offering career counseling services to individuals who seek employment at financial institutions; and • Management consulting activities on any subject to a financial institution and on financial, economic, accounting, or audit matters to any company.
Financial Institution	Refers to any institution the business of which is significantly engaged in financial activities, which may include but are not limited to: • Extending credit and servicing loans; • Lending, exchanging, transferring, investing for others, or safeguarding money or securities; • Insuring, guaranteeing, or indemnifying against loss harm, damage, illness, disability, or death. o The FTC has classified institutions of higher education as financial institutions for purposes of compliance with the Gramm-Leach-Bliley Act's safeguarding rule as such institutions process student loans.
Service Providers	Refers to all third parties who, in the ordinary course of institutional business, are provided access to customers' covered data and information. Service Providers may include, but are not limited to, business retained to store, transport, and/or dispose of covered data; collection agencies; and technology systems support providers.

Procedures

Scope of Program: Non-public Financial Information	A. The Program shall apply to any paper or electronic record maintained by the University that contains nonpublic financial information about an individual or a third party who has a relationship with the institution.

B. Such nonpublic financial information shall be kept confidential and safeguarded by the institution, its affiliates and service providers pursuant to the provisions of the Program.

Requirements of an Information Security Program

A. Program Coordinator
   1. The University's Security Information Program must include the designation of a Program Coordinator ("Coordinator") who shall be responsible for implementing the Program.
   2. The Coordinator may be a single employee as designated by the Program.
      a. In the alternative, the Program may designate several employees as Coordinators such that one employee serves as the institution's primary Coordinator who works in conjunction with departmental Coordinators who are responsible for oversight of safeguarding records in their departments in accordance with the University's Program.
   3. The Coordinator shall, at a minimum, perform the following duties:
      a. Consult with the appropriate offices to identify units and areas of the University with access to customers' nonpublic financial information and maintain a list of the same;
      b. Assist the appropriate offices of the institution in identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customers' nonpublic financial information and make certain that appropriate safeguards are designed and implemented in each office and throughout the institution to safeguard the protected data;
      c. Work in conjunction with the Office of Procurement and Contract Services to guarantee that all contracts with third party service providers that have access to and maintain nonpublic financial information of the institution's customers include a provision requiring that the service provider comply with the GLBA safeguarding rule;
      d. Work with responsible institutional officers to develop and deliver adequate training and education for all employees with access to customers' nonpublic financial information; and
      e. Periodically evaluate and monitor the effectiveness of the current safeguards for controlling security risks

by periodically verifying that the existing procedures and standards delineated in the Program are adequate.

B. Security and Privacy Risk Assessments
   1. The Program shall identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise of such information, and assess the sufficiency of any safeguards in place to control those risks.
   2. Risk assessments should include consideration of risks in each office that has access to customers' nonpublic financial information.
   3. The GLBA requires that the risk assessment section of the Program must, at a minimum, include consideration of the risks in the following areas:
      a. Employee training and management.
         1. A GLBA employee training program shall be developed by the Coordinator in conjunction with the human resources office and legal counsel, if necessary, for all employees who have access to individuals' nonpublic financial information, such as information technology/systems employees and those employees who use such data as part of their essential job duties.
         2. The training shall occur on a regular basis, as deemed appropriate by the Coordinator, and it shall include education on relevant policies and procedures and other safeguards in place or developed to protect nonpublic financial information.
      b. Safeguards of information systems/technology processing, storage, transmission and disposal (including network and software design).
         1. Programs should include safeguards so that network and software systems are reasonably designed to limit the risk of unauthorized access to nonpublic financial information.
      c. Methods to detect, prevent, and respond to attacks, intrusions, or other system failures.

C. Implementation of Safeguards
   1. The Program must include information regarding the design and implementation of information safeguards to control the risks identified through the risk assessment

described in the previous component, "B. Security and Privacy Risk Assessments."

2. The Program shall also include methods to regularly test or otherwise monitor the effectiveness of the safeguarding procedures.
    a. The Program's monitoring may include technology system checks, reports of access to technology systems, and audits.

D. Oversight of Service Providers and Contracts
1. The GLBA requires institutions to take reasonable steps to select and retain third party service providers that are capable of complying with the GLBA by maintaining appropriate safeguards for the customer information to which they have access.
2. The GLBA requires that the institution's current and potential service providers that have access to customers' nonpublic financial information maintain sufficient procedures to detect and respond to security breaches.
3. The Program must include a reference to the institution's duty to require, by contract, that all applicable third party service providers implement and maintain appropriate GLBA safeguards for customers' nonpublic financial information.

E. Evaluation and Revision of Program
1. The GLBA mandates that the University's Program be subject to periodic review, evaluation, and adjustment.
2. The Program must include a plan by which it will be evaluated on a regular basis and a method to revise the Program, as necessary, for continued effectiveness.

Assessment of the Information Security Program

The Coordinator, in conjunction with the appropriate administrators, shall assess the effectiveness of the Program annually.

1. The Coordinator shall make certain that necessary revisions to the Program are made at the time of the annual review to address any changes in the institutional organization that may affect the implementation and effectiveness of the Program.

Publication of the Information Security Program

A. To promote uniform compliance with the Program by all personnel employed by APSU and to achieve the University's duty to safeguard the confidentiality of customers' nonpublic financial information, the institution shall, at a minimum, display and disseminate the Program in accordance with the institution's standard distribution

methods.

B. The University's current Program shall be available upon request for review and copy at all times.

Links

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

Revision Dates

APSU Policy 4:041 – Issued: March 25, 2017

Subject Areas:

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

Approved

President: signature on file