STEPHEN F. AUSTIN
STATE UNIVERSITY
Office of the General Counsel

POLICY SUMMARY FORM

Policy Name: Gramm Leach Bliley Act Required Information Security

Policy Number: 14.4

Is this policy new, being reviewed/revised, or deleted? Review/Revise

Date of last revision, if applicable: April 14,2015

Unit(s) Responsible for Policy Implementation: Finance and Administration

Purpose of Policy (what does it do): Ensure the security and confidentiality of customer information, safeguard against unauthorized access of such data.

Reason for the addition, revision, or deletion (check all that apply):

☒ Scheduled Review ☐ Change in law ☐ Response to audit finding

☐ Internal Review ☐ Other, please explain:

Please complete the appropriate section:

Specific rationale for new policy:

Specific rationale for each substantive revision: Added section on reporting requirements; reference of alignment with policy 14.1 Information Security Management; minor wording changes

Specific rationale for deletion of policy:

Additional Comments:

Reviewers:

Judith Kruwell and Michaelyn Greene

Gramm Leach Bliley Act Required Information Security

Original Implementation: April 21, 2009
Last Revision: ~~April 14, 2015~~*April 24, 2018*

Overview

In conjunction with university policy 14.1 Information Security Management, Stephen F. Austin State University ~~’s~~ (university) adopts this information security program (program) to address the Standards *for*~~of~~ Safeguarding Customer Information *(*Safeguard*s* Rule*)* as mandated in 16 CFR 314 of the Gramm-Leach-Bliley Act (GLBA). As required by the GLBA, this program applies to customer financial information (~~“~~covered data~~”~~) *that* the university receives in the course of business.

Program Objectives~~:~~

- ~~1.~~ Ensure the security and confidentiality of customer information,
- ~~2.~~ Protect against any anticipated threats or hazards to the security of customer information, ~~and~~
- ~~3.~~ Protect against unauthorized access or use of such data or information in ways that could result in substantial harm or inconvenience to students, faculty, staff, and the university community.

Definitions~~:~~

Covered Data means all information required to be protected under the GLBA.

Customer information means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer (student, prospective student, parent, guardian, faculty, or staff), whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the university.

Information security program means the administrative, technical, or physical safeguards the university uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Nonpublic financial information means any information that meets any of the following criteria:

- Information a student or other third party provides in order to obtain a financial service from the university;
- Information about a student or other third party resulting from any transaction with the university involving a financial service; or
- Information obtained about a student or other third party in connection with offering a

financial service to that person.

Offering a financial service includes offering student loans, receiving information from a current or prospective student's parents as a part of a financial aid application, and other miscellaneous financial services as defined in 12 CFR 225.28.

Service provider means any person or entity that receives, maintains, processes or otherwise is permitted access to customer information through its provision of services.

Scope of the Program

The program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the university, whether in paper, electronic or other form that is handled or maintained by or on behalf of the university.

Elements of the Program~~:~~

Designate a Program Officer(s)

Oversight of the program will lie with the vice president for finance and administration. The vice president for finance and administration will designate a program officer with ~~overall~~ responsibility for overseeing the university's *customer* information security program and may designate other representatives of the university to assist in the coordination of the program. Any questions regarding the implementation of the program or the interpretation of this document should be directed to the vice president for finance and administration.

Identify and Assess Risk

The university intends, as part of the program, to undertake to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. In implementing the program, the program officer will establish procedures for identifying, and assessing such risks in each relevant area of the university's operations including:

- Employee training and management;
- Information systems*, including network and software design,* ~~and~~ information processing, *storage, transmission* and disposal; and
- Detecting, preventing and responding to attacks*, intrusions, or system failures*.

Design and Implement Safeguards

The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in *paper,* electronic, ~~paper~~ or other form. The program officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers

The university will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. The program officer will work with the Office of the General Counsel to develop and incorporate standard contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.

Program Review and Revision

The program officer is responsible for evaluating and adjusting the program based on the risk assessment activities *or on the results of testing and monitoring,* as well as material changes in the university's operations or other circumstances that may have a material impact on the program.

Reporting Requirements

The program officer, in coordination with the university information security officer, will report any data breach including unauthorized disclosure, misuse, alteration, destruction, or other compromise of information to the Department of Education on the day of detecting or suspecting an incident.

Cross Reference: 12 CFR 225.~~26~~*28*; 16 CFR 314; 16 CFR 313.3(n); Use of Electronic Information Resources (16.32); Computer & Network Security (14.2); Student Records (2.10)*; Information Security Management (14.1)*

Responsible for Implementation: Vice President for Finance and Administration

Contact for Revision: Vice President for Finance and Administration

Forms: None

Board Committee Assignment: Finance and Audit