Policy Number: 06-105
Last Revised: N/A

Security and Identity Theft Prevention Program

Purpose

This policy affirms that Stephen F. Austin State University (university) is committed to preventing identity theft through an information security program (program) that addresses the Standards for Safeguarding Customer Information (Safeguards Rule) as mandated in 16 CFR 314 of the Gramm-Leach-Bliley Act (GLBA). This policy is in addition to any other information security policies currently at Stephen F. Austin State University.

Persons Affected

All SFA employees are affected by this policy.

Definitions

Covered Data: All financial information received in the course of business that is required to be protected under the GLBA.

Customer information: 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.

Identity Theft: Fraud committed or attempted using the identifying information of another person without authority.

Information security program: 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.

Non-public financial information: 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: 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.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Red Flag Rules: Rules issued by the Federal Trade Commission (FTC) on November 7, 2007 regarding identity theft. These rules implement Sections 114 and 115 of the Fair and Accurate Credit Transactions Act and require certain policies and procedures be developed that are designed to detect, prevent and mitigate identity theft.

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

Policy

The program's objectives are to ensure the security and confidentiality of customer information and protect against any anticipated threats or hazards to the security of customer information.

The program applies to any record containing non-public 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.

Procedures

A. *Program Administration*

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 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. The program officer is also 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.

B. *Identifying and Assessing 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 detecting relevant red flags, and assessing risks in each relevant area of the university's operations including:

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

C. *Designing and Implementing 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, 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.

D. Responding to Fraudulent Activity

Once potentially fraudulent activity is detected, a rapid appropriate response can protect employees, students, and the university from damages and loss. An employee should gather all documentation related to the suspicious activity and report as outlined in the university Dishonest or Fraudulent Activities Policy (01-403) and Procedures for Identifying and Responding to Red Flags for Identity Theft Prevention.

E. Overseeing Service Providers

It is the responsibility of the university to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft and to provide adequate safeguards for customer information. 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.

F. 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 student information to the Department of Education on the day of detecting or suspecting an incident.

Related Statues or Regulations, Rules, Policies, or Standards

Fair and Accurate Credit Transactions Act of 2003;12 CFR 225.28; 16 CFR 314; 16 CFR 313.3(n); 16 CFR 681

UTS 118 Dishonest or Fraudulent Activities

SFA HOP 01-403 Dishonest or Fraudulent Activities
SFA HOP 06-101 Acceptable Use of Information Technology Resources
SFA HOP 06-107 Information Security Management
SFA HOP 01-301 Access to University Records

Red Flags Rule; Procedures for Identifying and Responding to Red Flags for Identify Theft Prevention Website

Responsible Executive

Vice President for Finance and Administration, Chief Information Officer, Director of Treasury and Student Business Services

Forms

None

Revision History

September 1, 2023 (original)