GRAMM-LEACH-BLILEY ACT

Overview

This document summarizes Southwest University at El Paso's information security program as mandated by the Federal Trade Commission's Safeguards Rule and the Gramm - Leach - Bliley Act ("GLBA"). The information security program is coordinated by the school director in alliance with the administration, financial aid, and IT directors. While these practices mostly affect the Information Technology department they may impact other areas of the university such as administration, registrars, financial aid, placement, advising and admissions departments. The purpose of this program as required by GLBA is to provide an outline to ensure ongoing compliance with federal regulations related to the program. This program is in addition to any other University policies and procedures that may be required pursuant to other federal and state laws and regulations, including Family Educational Rights and Privacy Act ("FERPA").

Scope of Program

Gramm – Leach – Bliley Act (GLBA) Requirements

GLBA mandates that the University/Institution (i) designate an employee(s) to coordinate the Program, (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of covered information, giving consideration to operations such as employee training and management, information systems, and potential system failures, attacks and intrusions, (iii) design and implement information safeguards to control the risks identified through risk assessment, (iv) oversee service providers and contracts, and (v) evaluate and adjust the Information Security Program periodically.

Designation of Representative(s)

Institutional administration (School Director and President) shall be responsible for coordinating and overseeing GLBA Program. The administrative team may designate other representatives of the University to oversee and coordinate particular elements of the when required. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the School Director.

Our Administrative team has assigned our director of Integrated Technology to review any security issues regarding IT related purposes. The IT director is responsible to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of account information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement an administrative, technical and physical safeguards program, regularly monitor and test the program and report to the School Director and/or President.

Risk Assessment and Safeguards

The University intends, as part of the Program, to (i) identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of nonpublic personal information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and (ii) assess the sufficiency of any safeguards in place to control these risks. The GLBA will work with all Data Gatekeepers (Financial Aid and IT directors) to identify potential and actual risks to security and privacy of information.

Each Data Gatekeepers will conduct a data security review, with guidance from the GLBA. IT will ensure that procedures and responses are appropriately reflective of those widely practiced at other national colleges.

The University has discontinued usage of social security numbers as student identifiers and now provide students Identification numbers. Social security numbers are considered protected information under both GLBA and the FERPA. By necessity, student social security numbers remain in the University student information system (Diamond D). The GLBA administration team and data gatekeepers will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances, if any, students are inappropriately being asked to provide a social security number. This assessment will cover University employees as well as subcontractors such as student loan billing and collection services.

IT will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

IT will develop plans and procedures to detect and prevent any attempted attacks, intrusions or other failures on central systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

Designing and Implementing Safeguards

The GLBCC will, on a regular basis, assist Data Gatekeepers in implementing 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.

This evaluation will include assessing the effectiveness of the University's current policies and procedures relating to system access, the use of the University's network, network security, documentation retention and destruction. The GLBA administrative team will also coordinate with IT to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems, implementing patches or other software fixes designed to deal with known security flaws.

Employee and Training Management

While the GLBA administrative team are ultimately responsible for ensuring compliance with information security practices, the GLBA administrative team will consult with relevant offices to evaluate the effectiveness of practices relating to access to and use of covered information. Employees with access to covered information typically fall into three categories: professionals in information technology who have general access to all university data, Data Gatekeepers who have access to specific systems, and those employees who use data as part of their essential job duties.

Oversight of Service Providers

The GLBA administrative team shall consult with those responsible for the procurement of third party services and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic personal information of students and other third parties to which they will have access. In addition, the GLBA administrative team will work with any providers to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. These standards shall apply to all existing and future contracts entered into with such third party service providers.

Review and Revision

This Program is subject to review and revision by the GLBA administrative team and its Gate Keepers, based on the risk assessment results, to ensure compliance with existing and future laws and regulations. Technology security should undergo quarterly review by IT. Other processes, such as data access procedures and training should undergo regular reviews by the GLBA administrative team and its Gate Keepers.

General Questions

Questions regarding the University's GLBA policy or regarding information security may be e-mailed to: mgutierrez@southwestuniversity.edu