Viterbo University
GLBA Information Security Program

Overview

This document summarizes Viterbo University's (the "Institution's") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm–Leach–Bliley Act ("GLBA"). In particular, this document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates by reference the Institution's policies and procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA and the Higher Education Act (HEA).

Designation of Representatives

The Institution's Vice President of Finance and Administration is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

Scope of Program

The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program

1. ***Risk Identification and Assessment.*** The Institution intends, as part of the Program, to undertake to identify and assess 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 other compromise of such information.

Internal and external risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

The Institution will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks.

Current safeguards implemented, monitored, and maintained by the Institution are reasonable, and in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the Institution. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity 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 Institution's operations, including:

- *Employee training and management*. The Program Officer will coordinate with representatives in the Institution's Human Resources and Financial Aid offices to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information (Section 483(a)(3)(E) of the Higher Education Act (HEA) restricts the use of FAFSA/ISIR data to the application, award, and administration of aid awarded under federal student aid programs, state aid, or aid awarded by eligible institutions). This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area, including Financial Aid Code of Conduct, Identity Theft Prevention Program, Policy on Reporting Suspected Fraudulent or Illegal Activity, PCI Credit Card Security Policy, and PCI Credit Card Processing Policy. New employees in the Registrar's Office, Business Office, and Financial Aid Office receive proper training on the importance and appropriate use/sharing of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also instructed in the proper use of computer information and passwords.

- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with representatives of the Institution's Instructional and Information Technology department to assess the risks to nonpublic financial information associated with the Institution’s information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution’s current polices and procedures relating to Appropriate Use of Technology and Records Retention Schedule. The Program Officer will also coordinate with the Institution’s Instructional and Information Technology department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws. Access to covered data and information is limited to those employees who have a legitimate business reason to access such information. Employees are instructed in controls and procedures to prevent providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. Each department responsible for maintaining covered data and information is instructed to take steps to protect that information from destruction, loss, or damage due to environmental hazards or technical failures.

- *Detecting, Preventing and Responding to Attacks*. The Program Officer will coordinate with the Institution’s Instructional and Information Technology and other relevant departments to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the Instructional and Information Technology department the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

2. ***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 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.

3. ***Overseeing Service Providers***. The Program Officer shall coordinate with those responsible for the third party service procurement activities among the Instructional and Information Technology department 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 financial information of students and other third parties to which they will have access. In addition, the Program Officer will work to ensure development and incorporation of 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.

4. ***Adjustments to Program.*** The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.