GLBA Safeguards Rule Information Security Program

Summary

This document provides a framework for the University's Information Security Program (ISP), which is required for compliance with the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (the Final Rule) pursuant to 16 CFR 314. Under the Final Rule, the University is required to develop, implement, and maintain a comprehensive ISP outlining the activities, policies, and programs in effect that serve to protect certain sensitive customer information.

Objectives

In accordance with the Final Rule, the objectives of the University's ISP are:

1. To safeguard the security and confidentiality of customer information;
2. To defend customer information from expected or reasonably foreseen threats; and
3. To protect customer information from unauthorized access where such information could be used to cause significant harm or inconvenience to the customer.

Scope of Information

The ISP as outlined in this document applies to any record containing *nonpublic personal information*, whether in paper, electronic, or other form, that is handled, maintained, or processed by or on behalf of the University or an affiliate. Such information is included in the scope of the ISP only if the information is obtained during the procurement or transaction of a financial product or service.

Nonpublic personal information refers to information:

i. Students, faculty, staff, or third-parties provide to the University in order to obtain a financial product or service,
ii. About students, faculty, staff, or third-parties as a result of a transaction with the University involving a financial product or service, or
iii. Otherwise obtained about students, faculty, staff, or third-parties in connection with providing a financial product or service to that individual.

Essentially, information covered under the scope of the ISP is financial information obtained from a financial product or transaction with the University or an affiliate that could be used to personally identify students, faculty, staff, or other third-parties.

Examples of such information include:

i. Account balance, payment history, and credit/debit card purchase information of students, faculty, staff, or other third-parties;
ii. The fact that students, faculty, staff, or other third-parties have obtained a financial product or service from the University;
iii. Information that students, faculty, staff, or other third-parties provide to the University or an affiliate(s) obtains while collecting on or servicing a credit account; and
iv. Any personal financial information the University or an affiliate collects through Internet "cookies."

Related Policies and Activities

The University has established policies and implemented various activities intended to ensure the protection and confidentiality of *nonpublic personal information* it has been provided. Policies and procedures listed below provide more detail on steps the University has taken to reasonably ensure customer information is safeguarded as stated in the Final Rule.

Cash Handling Procedures
Computer Use Policy
Credit Card Processing & Security Policy
Data Standards Manual
Inventory Procedures Manual
Key and Lock Guidelines
Mobile Device Security Policy
Network Password Policy
Network Security Policy
Remote Access Policy
User Account Management Policy

Elements of the University's ISP

Program Coordinator

The University's designated ISP Coordinator (Coordinator) is the Vice President for Finance and Administration. The Coordinator may select others to supervise certain elements of the ISP and may designate an employee to act in place of the Coordinator for the purposes of fulfilling the responsibilities set forth in the ISP. Questions regarding the ISP should be directed to the Coordinator or Qualified Individual.

Qualified Individual

The Qualified Individual for the University is the Director of Information Security. The University's Qualified Individual is the person responsible for overseeing, implementing, and enforcing the University's ISP. An annual ISP report will be provided to the VP of Information Technology for the University and to the Board of Trustees. This report will cover the risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how management responded as well as any recommended changes to the University's ISP.

Risk Identification and Assessment

Each University college/administrative unit is tasked with the identification and assessment of reasonably predictable risks, both internal and external, to the security and confidentiality of nonpublic personal information that could result in unsanctioned disclosure, misuse, modification, or disposal of such information. Additionally, each college/administrative unit is responsible for determining the sufficiency of safeguards in place to regulate the risks identified.

Finance and Administration offers resource materials to assist managers with evaluation of current information protection activities and anticipated risks in daily operations, including:

1. Employee Training and Management – reference materials for employees and managers describing procedures in effect governing access, use, etc. of customer records. Managers may use this information in evaluating current employee training efforts.

2. Information Systems – policies and practices from the Division of Information Technology (IT) designed to protect the University network. Managers may use this information in assessing procedures and/or processes and may contact IT should they need more information on technical safeguards related to IT policies.

3. Prevention, Detection, and Response to Systems Attacks and Failures – policies and practices published by IT on measures taken to protect the University network and University-owned devices and information from attacks. Managers may use this information to understand what steps have been taken to reasonably protect the University network and information from attacks and/or failures.

Developing and Implementing Controls

Each University college/administrative unit with customer information subject to the Final Rule is responsible for designing and implementing safeguards to ensure risks identified during the risk assessment process are properly controlled. Colleges/administrative units are also responsible for periodically testing or monitoring controls to ensure they are functioning as intended. Testing and monitoring may be achieved by periodically reviewing key policies, processes, and practices to ensure no covered information is compromised, ensuring employees are aware of and following critical information, and related information security practices.

Management of Affiliates and Third-Party Providers

The Coordinator or Qualified Individual will work the Office of the General Counsel (OGC) to ensure a standard provision(s) is included in contracts with third-party service providers that requires providers to develop and maintain safeguards aimed at reasonably ensuring the protection of nonpublic personal information. Additionally, the Coordinator, OGC, and Purchasing Office will together work toward the selection and retention of service providers who are capable of and committed to implementing appropriate safeguards.

Changes to Program

The Coordinator or Qualified Individual will evaluate and adjust the ISP as necessary based on the results of risks identified, assessments, and testing and monitoring activities, or when modifications are required due to significant changes in the University's operations or operating environment.

Effective Date

The University's ISP is effective June 12, 2018.
The University's ISP was revised on November 7, 2022.