The University of Vermont

OFFICE OF AUDIT AND COMPLIANCE SERVICES
UVM.EDU/POLICIES

UNIVERSITY OPERATING PROCEDURE

Title: Gramm-Leach-Bliley Information Security Program

Overview

The University takes seriously its responsibility to safeguard personal data and its obligation to comply with the various federal, state and international laws related to the protection of personal, sensitive or otherwise protected data for which it collects. One of these laws, the Gramm-Leach-Bliley Act ("GLBA") requires that the University implement an information security program designed to protect and safeguard all non-public information (NPI) which it has collected for the purpose of offering a financial product or service. The University has an institution level Information Security Policy and related Information Security Procedures which describe elements of the University's overall information security program and which includes the protection of NPI under GLBA. This UOP is intended to provide additional information as it specifically relates to GLBA and is not intended to override these institution level policies and procedures related to information security. As such, the institution level policies and procedures related to information supersede this UOP regarding issues of application and in the event of a conflict between this UOP and the institution level policies and procedures.

Applicability of the Procedure

This UOP applies to all University staff, faculty and third parties who have access to student financial data and who require the ability to access, use or disclose NPI as part of their job duties.

Definitions

Customer:	means any individual who receives a financial product or service from the University. Most often it will be a student or their parent(s)/legal guardian(s). It could also include spouses, faculty, staff or other third parties.
Gramm-Leach-Bliley Act (GLBA):	is also known as the Financial Services Modernization Act of 1999. GLBA is a federal law that requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. Through its lending programs, the University of Vermont is required to comply with GLBA for those areas of its operations related to this lending.
Non-Public Personal Information (NPI):	is personally identifiable information (PII, defined below) which is (i) provided by a customer to the University, (ii) provided by another financial institution to the University, or (iii) otherwise obtained by the University for the purpose of offering a financial product or service.

Examples of NPI include, but are not limited to:

- Financial Account Numbers (bank, credit card)
- Credit Rating/Credit Data
- Social Security Numbers
- Loan Documents/Payoff Amounts
- Tax Returns
- Asset Statements

Personally Identifiable Information (PII): is information that can be used by itself or in combination with other information to identify an individual.

Examples of PII include, but are not limited to:

- Name
- Physical Address
- Email Address
- Date of Birth
- Mother's Maiden Name
- Phone Number
- Social Media Account Name

Procedures

GLBA requires that the GLBA Information Security Program include the following elements. The University's procedures as they relate to these elements are as follows:

Element #1: Designate one or more employees to coordinate its GLBA information security program.

The Information Security Officer (ISO), the Chief Privacy Officer (CPO), the Registrar, and the Director for Student Financial Services (SFS) are designated as the individuals responsible for coordinating its GLBA information security program. The Associate Director for Student Financial Services has been designated as the individual with day-to-day oversight of the program.

Elements #2: Identify and assess the risks to customer information as it relates to the University's provision of financial products or services; Element #3: Evaluate the effectiveness of the current safeguards for controlling these risks; Element #4: Design and implement a safeguards program, and regularly monitor and test it.

The ISO will work with the Director for SFS and the Associate Director for SFS to identify risks to security and privacy of the University's financially related information systems. While the Information Security Office is primarily responsible for internal and external risk assessment of University systems including those that store NPI, all members of the University are responsible for safeguarding NPI.

The ISO, in consultation with the Director and Associate Director of SFS, the CPO and the Registrar, will conduct regular data security reviews of the University's financially related information systems and services. The Associate Director for SFS, in consultation with the Director for SFS, the ISO, CPO and the Registrar, will perform an annual risk assessment related to the handling of NPI that will include documentation of internal controls. As specified in the University's Information Security Procedures, management remains responsible for the review and identification other security risks, including the storage of paper records or other records that contain NPI data. Data Stewards are responsible for ensuring that University Information, including NPI, within their area of assigned responsibility is used with appropriate, controlled levels of access and with assurance of its confidentiality and integrity. The ISO, the Director of SFS, and the CPO are available to provide guidance to management and to Data Stewards during this process.

Access to the University's financially related information systems and services is provided on an as-needed basis Access is requested by the individual user's supervisor and approved by the Office of the Registrar. Access to the forms that contain student financial information is approved by the Office of Student Financial Services. The Registrar is responsible for ensuring that access to these forms is not granted without approval from SFS.

The CIO, in coordination with the ISO, is responsible for assuring physical security of the University's primary system that houses NPI as well as of the network that the University uses to access this system. During risk assessments of other University areas, the ISO will notify the Director of SFS and the CPO of other systems identified that contain NPI related to GLBA. As identified, the CIO, ISO, Director of SFS and the CPO will work together to develop a mitigation plan for any risks associated with those identified systems.

Element #5: Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information.

Through its Information Security Procedures, the University has developed standard language related to safeguards and their handling of NPI. This language is included in its contracts and agreements with service providers who may require access to NPI. As part of the University's procurement process, those contracts for technology that require access to NPI will undergo a security review.

Element #6: Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring

Policies are reviewed every three years unless otherwise specified. In addition to the regularly scheduled reviews, through its Information Security Procedures, the University requires that the CPO, the Chief Internal Auditor (CIA), and the ISO update the Policy as legal requirements and best practices evolve. In addition, as part of the Enterprise Risk Management program (ERM), risks are reviewed and mitigation plans developed using a risk-based approach.

Contacts

Questions concerning the daily operational interpretation of this UOP should be directed to the following:	
Title(s)/Department(s):	**Contact Information:**
Director for Student Financial Services	sfs.compliance@uvm.edu
Information Security Officer	iso@uvm.edu
Chief Privacy Officer	privacy@uvm.edu
Registrar	registrar@uvm.edu
Controller	(802) 656-2903

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- Code of Conduct and Ethical Standards
- Computer, Communication, and Network Technology Acceptable Use Policy
- Data Breach Notification Policy
- Information Security Policy
- Information Security Procedures
- NASFAA's Financial Aid Data Sharing White Paper
- Privacy Policy

Training/Education

Training related to this policy is as follows:

Training Topic:	GLBA Training		
Training Audience:	SFS Staff	**Delivered By:**	Student Financial Services
Method of Delivery:	Self-Study	**Frequency:**	Prior to Granting Access plus an Annual Refresher

Training Topic:	GLBA Training		
Training Audience:	All Non-SFS Employees With Access to Financial NPI	**Delivered By:**	Student Financial Services
Method of Delivery:	Self-Study	**Frequency:**	Prior to Granting Access

About This Procedure

Responsible Official:	Vice President for Enrollment Management	**Approval Authority:**	Vice President for Enrollment Management
Affiliated Policy Number(s):	V. 1.7.2	**Effective Date:**	May 29, 2019
Revision History:	None		