University of Vermont

OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

UNIVERSITY OPERATING PROCEDURE

FOR PRINTED USE ONLY

University Operating Procedures residing on UVM's Institutional Policy website are the most current versions available. If you are viewing a procedure anywhere else including in printed form or embedded on other websites, it may not be the most current.

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

Principle of Least Privilege: maintains that system users will be granted access to only those functions and data needed to perform their job duties and no more.

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: Designates a qualified individual responsible for overseeing and implementing the institution's or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a)).

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

Element #2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to the institution or servicer) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 C.F.R. 314.4(b)).

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, CPO and the Registrar, will perform an annual risk assessment related to the handling of NPI that will include documentation of internal controls and will present this to the ISO for evaluation. 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 with the principle of least privilege, as defined herein, applied. 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, and an appropriate level of access is granted at the request of the Registrar by Identity and Account Management (IAM, housed in the Information Security Office) and Enterprise Application Services.

The CIO, in coordination with the ISO and the Chief Technology Officer (CTO), is responsible for assuring physical security of the University's primary electronic 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 #3: Provides for the design and implementation of safeguards to control the risks the institution or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8).

1) The Director of SFS or their designee will perform an annual review to ensure that those with access to customer information are still active and that their access levels are appropriate. Role-based authorization will be applied in adherence to the principle of least privilege; roles are regularly reviewed and maintained. In addition to this annual review, there is a monthly review of access to verify that those with access remains appropriate.
2) The Responsible Official will periodically assess this policy and related procedures according to established university policy review cycles. Identified flaws, gaps, or areas of improvement will be addressed in a timely manner.
3) Any transfer or storage of NPI must employ data encryption methods approved by the Information Security Office.
4) Access to application and database development environments is controlled by network and host-based firewalls, host and application-level authorization schemes, and multifactor authentication. Per the Information Security Policy, Technology Managers who develop, maintain, or modify key applications relating to NPI must deploy adequate procedures for managing change control, separation of test and production environments, and separation of responsibilities and authorizations for staff involved in those functions.
5) Multifactor authentication is required to access or transmit NPI; this will be implemented uniformly as software lifecycles permit. Exceptions require ISO written pre-approval.
6) Data retention is consistent with the University Record Management and Retention Policy.
7) Log data required to audit for unauthorized access to customer information and related information systems is securely collected and maintained for an appropriate period of time; details are reserved.

Element #4: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

Regular testing and monitoring for effectiveness will be conducted in accordance with UVM's standard processes.

Element #5: Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 C.F.R. 314.4(e)).

1) Security training – Prior to receiving access to protected data, employees are required to review, and acknowledge comprehension of, relevant consumer information rules and regulations.
2) The Information Security Office is part of Enterprise Technology Services and works closely with colleagues in Enterprise Application Services and Database Administrators to ensure best practices are implemented and followed.
3) Professional Development funds are reserved to provide needed technology training in all areas of Enterprise Technology Services. Discussion forums are used to impart critical information in a timely manner. System Administrators work closely with application administrators to ensure patches and security updates are implemented in a timely fashion. The Cyber Security Incident Response Team (CSIRT) is activated for urgent and emergent issues.
4) All technology workers are engaged with appropriate knowledge resources to maintain currency in their areas and share threats and countermeasures through established communication channels. The CSIRT engages in regular readiness trainings and simulations.

Element #6: Addresses how the institution or servicer will oversee its information system service providers (16 C.F.R. 314.4(f)).

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 during the contracting process and, depending on the level of risk, may undergo a re-review during the contract renewal period.

Element #7: Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the information security program (16 C.F.R. 314.4(g)).

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.

Element #8: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the establishment of an incident response plan (16 C.F.R. 314.4(h)).

Incidents will be addressed according to UVM's information security policies and procedures. The CSIRT maintains an Incident Response Plan that incorporates a decision tree and checklist for declaration of an incident, activation of the CSIRT, determination of appropriate internal and external stakeholders, investigation, mitigation, reassessment, and reporting.

Element #9: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the requirement for its Qualified Individual to report regularly and at least annually to the Board of Directors or, if no such boad exists, to the senior officer responsible for the institution's information security program (16 C.F.R. 314.4(i)).

The Chief Information Officer shall report to the Audit Committee of the Board of Trustees at least annually on the status of the GLBA Information Security Program.

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:	Chief Information Officer	**Approval Authority:**	Chief Information Officer
Affiliated Policy Number(s):	None	**Effective Date:**	May 30, 2023
Revision History:	• May 29, 2019 • Posted as interim May 30, 2023. Responsible official officially changed from the Vice Provost for Enrollment Management to the Chief Information Officer. Interim status removed November 30, 2023.		