ADMINISTRATIVE POLICY
GRAMM-LEACH-BLILEY ACT
This policy pertains to employees.

Introduction

The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions, including colleges and universities that handle financial aid and other financial information, protect the privacy and security of customer information. This policy outlines the measures FVTC takes to comply with the GLBA and safeguard nonpublic personal information (NPI).

Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other workers at FVTC, including all personnel affiliated with third parties who handle NPI.

Definitions

- **Nonpublic Personal Information (NPI):** Any information that a student or other customer provides to obtain a financial product or service, or that results from a financial transaction or service provided to a student.
- **Customer:** Any student or individual who obtains a financial product or service from FVTC.
- **Service Providers:** Any third party that performs services for FVTC and handles NPI.

Information Security Program

FVTC will develop, implement, and maintain a comprehensive information security program designed to protect NPI. This program will include the following components:

1. **Designation of Representatives:**
    - Appoint a GLBA Compliance Officer responsible for coordinating the information security program.
    - The GLBA Compliance Officer will report in writing, regularly and at least annually, to the FVTC Board of Directors. The report shall include the following information:
        - The overall status of the information security program and compliance with this part
        - Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's response thereto, and recommendations for changes to the information security program
2. **Risk Assessment:**
    - Identify and assess the risks to NPI within each department handling such information.

- Evaluate the effectiveness of current safeguards for controlling these risks.
- Regularly review and update the risk assessment to address new or changing threats.

3. **Safeguarding Measures:**
   - Implement administrative, technical, and physical safeguards to control the identified risks. This includes:
     - Access controls to limit NPI access to authorized personnel only.
     - Encryption of NPI during storage and transmission.
     - Regular audits of systems and processes to ensure compliance with security standards.
4. **Employee Training and Management:**
   - Provide regular training to all employees who handle NPI on the importance of confidentiality and the proper handling of NPI.
   - Implement policies and procedures to ensure employees comply with the information security program.
5. **Oversight of Service Providers:**
   - Require service providers that handle NPI to implement and maintain appropriate safeguards.
   - Contractually obligate service providers to comply with GLBA requirements and FVTC's information security standards.
6. **Implementing Policies and Procedures:**
   - Develop, document, and implement comprehensive policies and procedures to manage and protect NPI.
   - Ensure policies cover the collection, processing, storage, transmission, and disposal of NPI.
   - Regularly review and update policies and procedures to address evolving security threats and legal requirements.
7. **Incident Response:**
   - Develop and maintain an incident response plan to address any breaches of NPI.
   - Define procedures for identifying, reporting, and mitigating the impact of a security incident.
   - Notify affected individuals and regulatory authorities as required by law.
8. **Monitoring and Testing:**
   - Regularly test the effectiveness of safeguards through audits and system checks.
   - Update the information security program based on the results of these tests and any new threats or vulnerabilities identified.
9. **Regular Review and Adjustment:**
   - Conduct annual reviews of the information security program to ensure continued effectiveness and compliance with GLBA.
   - Adjust the program as necessary to address changes in the institution's operations, technology, and external threats.

Adopted: 11/01/2024
Reviewed: 10/22/2024
Revised: NA