University Policy #600.04

COMPLIANCE WITH THE FEDERAL GRAMM-LEACH BLILEY ACT (GLBA)

Responsible Administrator: Office of the President
Responsible Office: Information Technology
Originally Issued: August 2025
Revision Date:
Authority: Office of the President

It is the policy of Claflin University to protect the security, confidentiality, and integrity of stakeholder information in compliance with the federal Gramm-Leach-Bliley Act (GLBA). In 1999, the GLBA safeguarded the confidentiality of customer information held by financial institutions, including banks, investment firms, and higher education institutions participating in Title IV federal student aid programs. In addition, in 2023, the United States Department of Education reinforced these requirements in General-23-09 which clarified how the Safeguards Rule applies to educational institutions. The key objectives of GLBA's Safeguards Rule are:

- To ensure the security and confidentiality of student information;
- To protect against potential threats to data integrity; and
- To prevent unauthorized access or misuse that may cause significant harm or inconvenience to students.

The GLBA requirements apply to Information, which is Nonpublic Personal Information (NPI) about a student or other third party who has a continuing relationship with Claflin University, where such information is related to provision of a financial service or product and that is maintained by or on behalf of the University. Examples include student loans, income tax information received from a student's parent when offering a financial aid package, bank and credit card account numbers, and income and credit histories.

Statement of Purpose

This policy outlines Claflin University's compliance with the Gramm-Leach-Bliley Act and the related regulation, the Safeguards Rule, which requires the University to develop, implement, and maintain a comprehensive written Information Security Program (ISP) to safeguard stakeholder financial information. The University has developed an ISP. The Program includes regular testing and monitoring of the effectiveness of key safeguards, including those to detect actual and attempted attacks on, or intrusions into the University's information systems.

Applicability

This policy applies to all University offices that collect, process, store, or transmit financial information related to students, employees, and other stakeholders including parents.

Definitions

1. **GLBA Information** - Sensitive, non-public, personally identifiable information including, but may not be limited to, an individual's name in conjunction with any of the following: social security number, credit card information, income and credit history, bank account information, tax return, asset statement. GLBA information includes both paper and electronic records.
2. **GLBA Offices** - Entities within the University that collect, process, store, or transmit financial information related to students, employees, and other stakeholders including parents. These offices include, but are not limited to, information technology, financial aid, fiscal affairs, auxiliary services, admissions, housing and residence life, and human resources.
3. **GLBA Services** - Examples include offering or servicing student and employee loans and receiving income tax information from a student's parent when offering a financial aid package.
4. **Office Representative -** a designated employee within a university office who is responsible for coordinating and overseeing that office's compliance with the GLBA. Supported by the Qualified GLBA Individual (the Interim Leader for Information Technology), the office representative also ensures that education and training is provided to personnel who works with GLBA information.
5. **Encryption** - The process of converting data into a coded format to prevent unauthorized access.
6. **Multi-Factor Authentication (MFA) -** Also known as 2-Factor Authentication, enhances security by combining two elements from three categories: e.g., something known (a password or PIN), something held (a hardware token or mobile device), and something identifying (e.g., biometric data, such as a fingerprint or retina scan.)
7. **Stakeholder** - Any individual (student, parent, faculty, staff, or other third party) with whom the University interacts, who receives a financial service from the University and who, in the course of receiving that service, provides the University with sensitive, non-public, personal information about themselves.

Procedures

A. Appointment of a Qualified Individual

Claflin University has designated the Interim Leader for Information Technology as the Qualified Individual to oversee, implement, and enforce its Information Security Program.

B. Information Security Program (ISP)

As previously noted, Claflin University has developed an information security program that identifies areas of risk and related appropriate safeguards. Safeguards are designed to reduce risk related to the handling of protected information. Claflin University's Information Security Program considers, but is not limited to, the following:

1. **Risk Assessments**
   - Conduct regular risk assessments to identify vulnerabilities in data handling processes.
   - Evaluate threats to financial data stored in university systems.
   - Develop mitigation strategies to address identified risks.

2. **Access Controls**
   - Access to the University's IT systems is based on a user's job function.
   - An annual comprehensive review is conducted to ensure that users retain only necessary access to sensitive information.
   - Access controls are reviewed and as necessary, adjusted after significant system changes, personnel changes, and/or security incidents.

3. **Data Inventory**
   - Maintain an inventory of data to track where information is collected, stored, and transmitted.
   - Classify data based on sensitivity to apply appropriate security measures.
   - Update data inventory annually.

4. **Encryption of Information**
   - Encryption is used to protect confidential data in use, in transit, and at rest.
   - Encryption methods are reviewed annually.

5. **Multi-Factor Authentication (MFA)**
   - Whenever technically possible, information technology systems require strong, complex, and unique passwords reinforced by the use of MFA.
   - Passwords must be updated if they are reused or show signs of being stolen, exposed, or otherwise compromised.

6. **Activity Logging**
   - Where feasible, access to sensitive areas should be logged, either through electronic systems or manually, to track entry and exit activity.
   - Dependent upon the University's resources, secure areas should be configured with video surveillance or other security measures to detect and deter unauthorized access.
   - Logs should be retained for a minimum of six months.

7. **Oversight of Third-Party Service Providers**
   - Third-party service providers at Claflin University are subject to a security risk review prior to entering into an agreement and on a regular basis afterward.
   - As the Qualified GLBA designee, the Interim Leader for Information Technology will review the security controls that a third- party provider has in place to ensure that standards, policies, and practices are consistent with applicable state and federal regulations as well as Claflin University policies.
   - Vendors who refuse to disclose security controls and practices or otherwise indicate a lack of consistent safeguards for information technology risk management shall be barred from accessing, storing, processing, or otherwise handling University protected data.

8. **Reporting of Security Incidents and Response**
   - Faculty, staff, student workers, and third-party vendors must immediately report any actual or suspected security incidents involving unauthorized access, disclosure, loss, or misuse of data.
   - If appropriate, investigation of the incident will begin.

9. **Review/Analysis of System or Network Changes**
   - Implement firewalls and intrusion detection systems to safeguard and monitor system and network integrity.

C. Employee Training and Education

Claflin University requires ongoing training and education to employees who handle information governed by the GLBA. As the GLBA Qualified Individual, the Interim Leader for Information Technology, will ensure that applicable office designates a GLBA representative. In turn, the representative with the support of the Qualified Individual are responsible for educating, facilitating, and enforcing compliance with GLBA information security policies and practices.

D. Compliance Monitoring

The first internal audit to ensure compliance with GLBA requirements will be conducted no later than two years after the implementation of this policy; thereafter, periodic audits will be conducted.