

Gramm-Leach-Bliley Act (GLBA)

Overview

The Gramm-Leach-Bliley Act (GLBA) is a federal law that applies to financial institutions and establishes requirements for protecting the privacy and security of consumer financial information. For higher education institutions, the law governs how student financial records—such as tuition payment information and financial aid records containing personally identifiable information (PII)—are collected, stored, accessed, and used.

Background

The GLBA requires financial institutions to protect the privacy, security, and confidentiality of customer information. Because colleges and universities participate in financial activities, the Federal Trade Commission (FTC) classifies higher education institutions as financial institutions under GLBA regulations.

The law includes specific requirements regarding the protection of consumer financial information. Under regulations issued in May 2000, colleges and universities that comply with the Family Educational Rights and Privacy Act (FERPA) are considered compliant with the GLBA Privacy Rule. However, institutions are also subject to the GLBA Safeguards Rule, which requires administrative, technical, and physical protections for customer information.

The Safeguards Rule requires institutions to establish and maintain a comprehensive Information Security Plan designed to protect the confidentiality and integrity of customer information. The plan must:

- Ensure the security and confidentiality of customer records and information;
- Protect against anticipated threats or hazards to the security or integrity of records; and
- Prevent unauthorized access to or use of information that could result in substantial harm or inconvenience to customers.

GLBA Requirements

GLBA regulations include:

- **Privacy Rule (16 CFR 313)**
- **Safeguards Rule (16 CFR 314)**
- **Pretexting Provisions / Pretexting Rule (15 U.S.C. § 6821) — prohibits obtaining customer information under false pretenses**

Both rules are enforced by the Federal Trade Commission (FTC) for higher education institutions.

Privacy Rule

The GLBA Privacy Rule regulates the collection, use, and disclosure of nonpublic personal information between financial institutions and their customers. Institutions that comply with FERPA are generally considered compliant with this rule.

Safeguards Rule

The Safeguards Rule requires institutions under FTC jurisdiction to implement measures to secure customer information. Institutions must also ensure that affiliates and third-party service providers maintain appropriate safeguards for any customer information they access or manage.

Under this rule, Angeles College must develop, implement, and maintain a comprehensive information security plan containing administrative, technical, and physical safeguards appropriate to:

- The size and complexity of the institution;
- The nature and scope of institutional activities; and
- The sensitivity of customer information maintained by the institution.

These safeguards must:

1. Ensure the security and confidentiality of customer records and information;
2. Protect against anticipated threats or hazards to the security or integrity of records; and
3. Protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to customers.

Pretexting Provisions

The GLBA Pretexting Provisions prohibit obtaining or attempting to obtain customer financial information through false pretenses, including fraudulent statements, impersonation, or deceptive practices. Angeles College must implement measures to detect, prevent, and respond to social engineering, phishing, impersonation, and other fraudulent attempts to access customer information.

To support compliance, the institution should:

- Train employees to recognize and report suspicious requests for information;
- Verify the identity and authorization of individuals requesting access to customer information;
- Establish procedures for handling sensitive information securely; and
- Maintain safeguards to prevent unauthorized disclosure of customer records and information.

Protecting Student Information

Under the Program Participation Agreement (PPA) with the Department of Education and the Gramm-Leach-Bliley Act (Public Law 106-102), Angeles College is required to protect student financial aid information, particularly information provided by the Department of Education or obtained in support of federal student aid programs.

To comply with GLBA requirements, the institution must:

- Develop, implement, and maintain a written information security program;
- Designate employee(s) responsible for coordinating the information security program;
- Identify and assess risks to customer information;
- Design and implement safeguards to control identified risks;
- Select service providers capable of maintaining appropriate security safeguards; and
- Periodically review and update the information security program.

The School Administrator (or designee), Information Security Officer (ISO) and Information Technology Specialist are responsible for evaluating and documenting the institution's security posture and ensuring timely remediation of identified deficiencies.

Procedures

1. Employee Responsibilities and Access Controls

The following requirements apply to all personally identifiable financial records maintained by the institution and are intended to protect the confidentiality, integrity, and security of customer information.

a. Authorized Access

Employees are granted access only to the information necessary to perform their job responsibilities. Access to additional resources requires authorization. Employees may access customer information solely on a legitimate "need-to-know" basis.

b. Protection of Access Credentials

Access privileges are assigned according to job duties and responsibilities. Employees are responsible for safeguarding all methods of access, including usernames, passwords, keys, and identification credentials. Sharing login credentials or allowing unauthorized access is prohibited.

c. Proper Use of Information

Employees must not knowingly alter, destroy, misuse, or improperly disclose customer information.

d. Secure Transmission of Information

Employees are responsible for ensuring that customer information is released only in an authorized and secure manner. This includes:

- Verifying the identity of individuals requesting information;
 - Using password-protected attachments or encrypted email when transmitting confidential information; and
 - Following institutional procedures for secure data handling.
-

2. Security Requirements

Personally identifiable financial records and information must be maintained in secure physical locations with controlled access. Institutional computers, servers, and information systems must have appropriate physical and electronic safeguards based on the sensitivity of the information processed or stored.

3. Audit Requirements

The Angeles College Information Security Officer (ISO) and Information Technology (IT) Specialist shall conduct an annual risk assessment. The results of the assessment shall be reported annually to the School Administrator(s) and the GLBA Compliance Coordinator, and shared during the Annual Advisory Board meeting.

4. Program Administration

a. Oversight

Responsibility for developing, implementing, and maintaining the GLBA Information Security Program rests with the GLBA Committee. Committee membership includes:

- Information Technology (IT) Specialist
- GLBA Compliance Coordinator (Associate School Administrator)
- Information Security Officer (ISO) (Registrar)
- School Administrator or designee

Committee members are responsible for supporting annual risk assessments within their respective departments. The AC Information Security Officer and Information Technology (IT) Specialist will report status to the School Administrator and GLBA Compliance Coordinator at least annually.

b. Committee Responsibilities

GLBA Committee members oversee implementation of GLBA-related activities and serve as primary contacts for department administrators. The Information Security Officer (ISO) and Information Technology (IT) Specialist is responsible for coordinating institution-wide compliance efforts and collaborating with legal counsel under the supervision of School Administrator or GLBA Compliance Coordinator (Associate School Administrator) as necessary.

c. Training Requirements

Employees with access to customer information or information systems subject to GLBA shall complete mandatory security and privacy awareness training. Training will be conducted periodically, as needed, to reinforce institutional security practices and compliance obligations.

5. Service Provider Requirements

When the College contracts with third-party service providers that access or manage personally identifiable financial information, the College will take reasonable steps to ensure such providers maintain appropriate safeguards.

These steps include:

1. Requiring service providers to maintain policies and procedures that protect the security and confidentiality of customer information; and
 2. Including contractual provisions requiring service providers to implement appropriate safeguards and use customer information only for authorized contractual purposes.
-

Definitions

Customer

An individual who obtains a financial product or service from the institution primarily for personal, family, or household purposes and maintains an ongoing relationship with the institution. Examples may include students receiving institutional loans, payment plans, or financial aid services.

Customer Information

Nonpublic personal information related to an individual who receives financial products or services from the institution. Examples include:

- Tuition payment information;
- Financial aid records;
- Student loan information; and
- Any financial records associated with institutional credit or payment arrangements.

Customer information remains protected under GLBA even if the individual ultimately does not receive financial aid or credit services.

Service Provider

Any person or entity that receives, maintains, processes, or is otherwise permitted access to customer information while providing services to the College.