

# Safeguard Rules Under the Gram-Leach-Bliley Act



ANTIOCH  
COLLEGE

<b>Policy Number:</b>	<b>Responsible Office:</b> Human Resources	<b>Governing Body:</b> College Council	<b>Last Review Date:</b> 11/29/2023
<b>Scope:</b> The policy applies to any records containing “nonpublic personal information” about a student or other individual who has a continuing relationship with the College, whether the record is in paper, electronic, or other form, and which is handled or maintained by or on behalf of Antioch College.			

## I. Introduction

The College has adopted policies and procedures for the purpose of safeguarding the privacy of a category of customer information defined as non-public personal information (NPI) which it may receive pertaining to its students and employees, in compliance the Gramm-Leach-Bliley Act (GLBA or the Act), as may be amended, and with other applicable regulations (e.g. the Federal Trade Commission’s Safeguards Rule and Financial Privacy Rule).

Under the GLBA, the College is required to implement safeguards to ensure the security and confidentiality of certain NPI that is obtained when the College offers or delivers a financial product or service to an individual for personal, family, or household purposes, with particular attention to information provided to the College by the Department of Education or information obtained by the College in support of the administration of the Title IV federal student financial aid programs authorized under Title IV of the Higher Education Act, as amended.

The College must implement an information security program that incorporates administrative, technical, and physical safeguards appropriate to its size and complexity, nature and scope of activities, and sensitivity of NPI at issue. The contents of this webpage summarize information related to this required information security program and provide links to obtain more information. Guidance relating to administrative, technical and physical security of NPI is identified in the College document entitled, GLBA Information Security Program.

## II. Objectives

This policy sets the standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of information covered by applicable provisions of the Gramm-Leach-Bliley Act (GLBA). This policy describes measures taken by Antioch College to

- Ensure the security and confidentiality of covered information
- Protect against any anticipated threats to the security of these records
- Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm.

## III. Requirements

- Designating an employee(s) to coordinate the information security program.
- Performing a risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (including NPI) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessing the sufficiency of any safeguards in place to control these risks. At minimum, the risk assessment must include consideration of risk in each relevant operational area, including:
  - Employee training and management.
  - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal.
  - Detecting, preventing, and responding to attacks, intrusions, or other systems failures.
- Implementing information safeguards to control identified risks and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures.
- Overseeing service providers by taking reasonable steps to select and retain providers capable of maintaining appropriate safeguards for NPI and requiring them by contract to implement and maintain such safeguards.
- Evaluating and adjusting the information security program in light of the results of the required testing/monitoring, any material changes to operations or business arrangements, or any other circumstances that may have a material impact on the program.

#### **IV. Policy and Process**

The goals for this program are as follows:

To ensure employees have access only to the relevant data needed to conduct college business;

To ensure the security and confidentiality of customer records and information;

To safeguard and prevent unauthorized access to personally identifiable financial records and information maintained by the college;

To comply with existing college policies, standards, guidelines and procedures; and

To comply with applicable federal, state and local regulations.

#### **V. GLBA Information Security Program**

GLBA Information Security Program outlines safeguards the College follows to secure nonpublic personal information to ensure compliance with the GLBA. GLBA Information Security plan includes 7 elements that institutions with fewer than 5,000 customers must follow:

- Identify designated qualified individuals responsible for overseeing and implementing the institution's information security program and enforcing the information security program in compliance with (16 CFR 314.4(a)).
- 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 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 CFR 314.4(b)).

- Provides for the design and implementation of safeguards to control the risks the institution identifies through its risk assessment (16 CFR 314.4(c)(1)). Safeguards that information security program must address are:
  - Implementation and periodical review of access controls
  - Periodic inventory of data, noting where it's collected, stored, or transmitted
  - Encryption of customer information on the institution's system and when it's in transit
  - Assessment of apps developed by the institution
  - Implementation of multi-factor authentication for anyone accessing customer information on the institution's system
  - Disposal of customer information security
  - Anticipation and evaluation of changes to the information system or network
  - Maintenance of logs of authorized users' activity and assess unauthorized access.
- Provides for the institution to regulatory test or otherwise monitor the effectiveness of the safeguards it has implemented
- Provides for the Implementation of policies and procedures to ensure that personnel are able to enact the information security program.
- Addresses how the institution will oversee information system service providers
- Provides for the evaluation and adjustment of the information security program based on the results of the required testing and monitoring.

## **VI. Policies supporting GLBA Safeguards Rules**

- [Policy 02.046 Use of Communication and Computer Systems](#)
- [Policy 02.054 Confidential College Information](#)
- GLBA Information Security Program