Title: **Gramm-Leach-Bliley Information Security Program Policy**

□ Initial Action: August 7, 2023
□ Board Action: 23-045
□ Last Revised:
Policy: New
Procedure: New
□ Last Reviewed:
□ Effective:
□ Next Review: August 2026
□ Responsibility: Chief Information Officer

POLICY

This policy describes Cecil College's (the "College")) information program policy mandated by the Federal Trade Commission's Safeguard Rule (16 CFR 314) and the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (collectively the "GLBA"). This mandate requires institutions of higher education to develop, implement and maintain safeguards to protect the security, confidentiality, and integrity of customer financial records and related non-public personal information. Certain GLBA designated non-public personal financial information is protected under other federal and/or state laws which also require the securing and safeguarding of data. Accordingly, this information security program incorporates and is in addition to institutional policies and procedures required by other federal and state laws and regulations, including, without limitation, the Family Educational Rights and Privacy Act ("FERPA").

SCOPE

This policy applies to all College staff, faculty, and third parties who have access to student financial data and who require the ability to access, use or disclose non-public personal financial information as part of their job responsibilities.

DEFINITIONS

"Consumer" means an individual who obtains or has obtained a financial product or service from the College that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

"Covered Data" means (i) non-public personal financial information about a Customer and (ii) any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any non-public personal financial information. Examples of Covered Data include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable financial information (e.g., names of students with outstanding loans). Covered Data is subject to the protections of GLBA even if the Customer ultimately is not awarded any financial aid or provided with a credit extension. Covered Data does not include aggregated personal information that has been de-identified or anonymized.

*"*Customer*"* means any consumer (i.e., student, parent, faculty, staff, or other third party with whom the College interacts) who receive a Financial Service from the College for personal, family or household reasons that results in a continuing relationship with the College.

"Customer Information" means any record containing non-public personal information about a customer of the College, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the College or its affiliates. Customer Information includes information obtained as a result of providing financial services to a student (past or present).

"Financial Service" includes offering or servicing student loans, receiving income tax information from a student or a student's parent(s) or guardian(s) when offering a financial aid package, reviewing credit reports in connection with providing a loan to a student or prospective student, engaging in debt collection activities, and leasing real or personal property to students for their benefit.

"Non-Public Personal Information" (NPI) means any personally identifiable financial information and other personal information, not otherwise publicly available, that the College has obtained from a customer in the process of offering a financial product or service; such information provided to the College by another financial institution; such information otherwise obtained by the College in connection with providing a financial product or service; and any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. Examples of personally identifiable financial information include, but are not limited to, names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers (all in both paper and electronic form).

"Service Provider" means any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Data through its direct provision of Financial Services to the College. This includes software-as-a-service providers who contract with the College to receive Covered Data for the delivery of Financial Services. Service Providers also include any person or entity that administers any aspect of the College's participation in U.S. Department of Education Title IV programs.

Additional definitions, where applicable, are found in 16 CFR part 314.2.

By way of example, the type of Covered Data regulated by the GBLA includes the following:

1. Information provided by an applicant or student to obtain a loan or extension of credit from the College, a private lender, or the federal government;
2. Information provided by a student to regularly receive refunds or make payments by wire transfer or debit card;
3. Information from a consumer report regarding a student to receive a loan;
4. Information from an employee or student to license real property from the College;
5. Account balance information, payment history, overdraft history, credit or debit card purchase information;

6. Any information provided by a student in connection with collecting on or servicing an account;
7. Personal information collected through an internet cookie for the provision of Financial Services (as defined above) by the College.

The following offices within the College may handle Covered Data in the delivery of Financial Services:

1. Student Services & Enrollment Management
2. Academic Programs
3. Finance & Administration
4. Foundation & Alumni Development
5. Information Technology

PROGRAM REQUIREMENTS

Element 1: Designation of Qualified Individual Responsible for Overseeing and Implementing Program

The Chief Information Officer (CIO) is the designated individual responsible for: (1) coordinating the GLBA information security program (the "Program"), (2) identifying internal and external risks to the security and confidentiality of Covered Data and evaluating current safeguards, (3) designing and implementing safeguards to control the identified risks and regularly test and monitor the effectiveness of these safeguards, and (4) evaluating the effectiveness of the Program.

The CIO shall also designate an appropriate individual(s) to serve as the College's Program Coordinator(s), who will serve as the primary resource and liaison with College divisions, departments, and Service Providers for addressing issues related to the GLBA Safeguards Rule and disseminating relevant information and updates.

Element 2: Risk Assessment

The CIO will work with the Vice President for Student Services and the Vice President for Finance to identify risks to security and privacy of the College's financially related information systems. While the IT Division is primarily responsible for internal and external risk assessment of College systems, including those that store NPI, all members of the College are responsible for safeguarding NPI.

The CIO, in consultation with Vice President for Student Services and the Vice President for Finance, will conduct annual information security risk assessments to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Covered Data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of information and the sufficiency of safeguards in place to control these risks. the following internal and external information security risks include, but are not limited to:

- Unauthorized access of Covered Data and information by someone other than the owner of the Covered Data

- Compromised system security because of system access by an unauthorized person of data during transmission
- Loss of data integrity
- Physical loss of data in the event of a disaster
- Errors introduced into the system
- Corruption of data or systems
- Management of account users in systems maintained by the College and service providers
- Unauthorized access of Covered Data by employees
- Unauthorized requests for Covered Data
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of Covered Data through third parties

The CIO, or designee, will monitor appropriate cybersecurity advisory literature for identification of risks in the future and ensure that information security risk assessments are performed periodically in the future.

Element 3: Safeguards to Control Risks Identified Through Risk Assessment

1. Access control and limiting access only to authorized users and the information they need to perform their duties and functions is the responsibility of the appropriate Vice President, department head and designated IT employees. Access is reviewed at least annually in consultation with the appropriate Vice President, department head, human resources, and CIO.
2. The IT division is responsible for identifying and managing the data, personnel, devices, systems, and facilities involved. An up-to-date inventory is maintained.
3. The appropriate Vice President and department head is responsible for ensuring that employees are encrypting all customer information in transit over external networks and at rest.
4. The IT division employees secure development practices for any applications in use.
5. Multi-factor Authentication (MFA) is required for any employee accessing information systems managed by the College's IT division.
6. The appropriate Vice President and department head is responsible for implementing procedures for secure disposal no later than two years after the last date the information is used. The appropriate Vice President is responsible for reviewing their division's data retention policies.
7. The CIO and appropriate Vice Presidents are responsible for adopting procedures for change management.
8. The IT division is responsible for implementing procedures and controls to monitor and log the activity of authorized users and detect unauthorized access.

Element 4: Monitoring Effectiveness of Implemented Safeguards

Regular testing and monitoring for effectiveness, including annual penetration testing, will be conducted in accordance with the IT division's standard processes and will be updated as required by evolving practices.

Element 5: Implementation of Policies and Procedures

References and/or background checks (as appropriate depending upon position) of new employees working in areas that have access to Covered Data are performed. New employees who handle Covered Data receive proper training on the importance of confidentiality of student records, student financial information and all other Covered Data, and the proper use of computer information and passwords. Thereafter, all employees are required to complete annual training in cybersecurity and FERPA to ensure compliance. Cybersecurity awareness training also includes controls and procedures to detect and identify ransomware, phishing and social engineering tactics to prevent employees from providing Covered Data to an unauthorized individual. These training efforts minimize risk and safeguard Covered Data and information. Security updates are regularly distributed to all employees to raise awareness and test vulnerability to social engineering tactics.

Element 6: Oversight of Information System Service Providers
GLBA requires the College to take reasonable steps to select and retain Service Providers who maintain appropriate safeguards for Covered Data by contractually requiring Service Providers to implement and maintain such safeguards. Effective FY24, the College IT division will review and approve a Higher Education Community Vendor Assessment Toolkit (HECVAT) prepared by a Service Provider who has or will have access to Covered Data, to ensure that the Service Provider's contracts contain appropriate terms to protect the security of Covered Data. Functional offices are responsible for managing user accounts by removing users when their access to Covered Data is terminated. The CIO shall periodically reassess the continued adequacy of safeguards provided by Service Providers to Covered Data based upon the risks presented.

Element 7: Evaluation and Adjustment of Policies
Policies are reviewed annually and updated as legal requirements and best practices evolve.

Element 8: Incident Response Plan
The College's Incident Response Plan (IRP) shall be reviewed annually by the CIO. Incidents will be addressed according to the College's (IRP). A decision tree and checklist for the declaration of an incident, determination of appropriate internal and external stakeholders, investigation, mitigation, reassessment, and reporting are included in the IRP.

Element 9: Information Security Program Annual Report to Board of Trustees
The CIO shall report to the Board of Trustees at least annually on the status of the GLBA Information Security Program