BROOKDALE COMMUNITY COLLEGE
COLLEGE REGULATION

4.7004R Gramm-Leach-Bliley Act (GLBA) Regulation

I. Title of Regulation

Gramm-Leach-Bliley Act (GLBA) Regulation

II. Objective of Regulation

This Regulation outlines the College's application of GLBA requirements.

III. Authority

Board of Trustees Bylaw 1.3054; Policy 4.7002 Information Security Program; Pub. L. No. 106-102, codified 15 U.S. Code 6801 et. seq.

IV. Regulation Statement

The Gramm-Leach-Bliley Act (GLBA), a U.S. federal law enacted in 1999, affects any institution that provides a "financial service." Colleges and universities fall under the GLBA as part of student and alumni financial services and processes. The GLBA requires colleges and universities to provide a privacy notice to students and restrict the non-public personal information they share about students with third parties. It also requires institutions to implement thorough administrative, technical, and physical information safeguards.

Brookdale Community College's ("the College") written Information Security Program ("the InfoSec Program") Regulation (4.7002R) addresses the administrative, technical, and physical information safeguards mandated by the Federal Trade Commission's Safeguards Rule of the GLBA.

1. Applicability

The GLBA applies to any record containing non-public financial information about a student or other third party who has a relationship with the College, whether in paper, electronic, or other form, which is handled or maintained by the College or on behalf of the College or its affiliates.

2. Key Definitions

Non-public financial information (NPI) means any information:

(i) a student or other third party provides in order to obtain a financial service from the College,
(ii) about a student or other third party resulting from any transaction with the College involving a financial service, or

(iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

A ***financial service*** is defined by federal law to include, but not be limited to, such activities as the lending of money; investing for others; providing or underwriting insurance; giving financial, investment, or economic advisory services; marketing securities and the like.

Institutional Data is defined as any Class 1 or Class 2 information (as defined by the College's Data Classification and Permitted Use Regulation 4.7003R) handled, stored, transferred, or utilized related to the College's organizational / institutional functions, students, employees, or constituents.

3. Roles and Responsibilities

3.1 Responsibilities: The College's Vice President of Finance and Operations (VPFO) and Chief Information Officer (CIO) are responsible for coordinating and overseeing the College's InfoSec Program; GLBA is a component of that program.

3.2 Risk Identification and Assessment: As part of the InfoSec Program, the College will identify and assess external and internal risks to the security, confidentiality, and integrity of NPI. This identification and assessment includes:

- ***Audits****:* On a routine basis, the College will perform audits for areas affected by the GLBA to assess risks. The CIO will work with departments on any items that need remediation.

- ***Employee Training and Management:*** In addition to the general information security training that all staff members are required to complete on a yearly basis, staff in the College's Financial Aid, Financial Operations, and Continuing and Professional Services areas will also be required to review the College's GLBA Regulation, Release of Academic and Demographic Data About Students Regulation ("FERPA," 6.1504R), and any departmental procedures relevant to the GLBA. Annual certification of department compliance will be provided by the appropriate department heads to the VPFO and CIO.

- ***Information Systems and Detecting, Preventing, and Responding to Attacks:*** The College will identity reasonably foreseeable risks to information systems and address detecting, preventing, and responding to attacks through the procedures outlined in the College's InfoSec Program Regulation (4.7002R).

3.3 Designing and Implementing Safeguards: The CIO will work with departments to implement safeguards to control the risks identified through the routine audit process mentioned above.

3.4 Overseeing Service Providers: As part of the College's third-party Institutional Data safeguarding process, and under the direction of the VPFO, all service providers that handle, store, transmit, or receive Institutional Data must incorporate language into the College's contracts stating that the service provider will protect the College's Institutional Data according to commercially acceptable standards and no less rigorously than it protects its own data. For service providers or vendors that provide Software-As-A-Service solutions (hosted solutions) and handle, store, transmit, or receive Institutional Data, the College also requires inclusion of an InfoSec contract clause which will be reviewed by the Executive Associate Legal Services, the CIO, and the VPFO.

3.5 Adjustments*:* The VPFO and CIO are responsible for evaluating and adjusting the GLBA Regulation based on the risk identification and assessment activities undertaken, as well as any material changes to the College's operations or other circumstances that may have a material impact upon it.

5. Review Cycle

This Regulation will be reviewed and updated as needed, at least annually.

6. Compliance and Enforcement

As described in the InfoSec Program Regulation (4.7002R), whenever a faculty member, staff member, contractor, student, or third-party is found to be negligent in, or have a blatant disregard for, compliance with the InfoSec Program or an approved security compliance standard, the College's first recourse will be to promptly notify the offender via a written warning. Additional infractions will incur progressive discipline. The College reserves the right to consider certain single incidents of non-compliance to be so harmful as to immediately rise to the level of more serious disciplinary consequences, up to and including a termination of employment, expulsion, or termination of contract.

V. Responsibility for Implementation

The President.

The VPFO and CIO are responsible for monitoring compliance with this Regulation and reporting instances of non-compliance to College's Senior Leadership Team stakeholders.

Related Policy; https://www.brookdalecc.edu/about/board-of-trustees/college-policies/4-0000- business-finance/4-7002-information-security-program/

Approved by Brookdale's Data Standards and Information Security IT Governance Committee on 9/9/2020

Approved by Brookdale's Information Technology Steering Committee on 10/8/2020

Approved by the Senior Executive Leadership Team on 1/6/2021

Approved: President, 1/6/2021