BROOKDALE COMMUNITY COLLEGE
COLLEGE REGULATION

4.7003R Data Classification and Permitted Use Regulation

I. Title of Regulation

Data Classification and Permitted Use Regulation

II. Objective of Regulation

This Regulation outlines the College's Data Classifications and guidelines for the permitted use of Institutional Data.

III. Authority

Board of Trustees Bylaw 1.3054; Policy 4.7002 Information Security Program

IV. Regulation Statement

Information technology and data constitute valuable assets for Brookdale Community College ("the College"). As part of the College's information security program ("the InfoSec Program," Policy 4.7002), in order to protect the security, confidentiality, and integrity of the College's data from unauthorized access, modification, disclosure, transmission, or destruction and to comply with applicable state and federal laws and regulations, all of the College's data is now classified into security levels. Appropriate standards and controls are included in these classifications that pertain to the usage of data at the various levels. All Institutional Data (defined as any information handled, stored, transferred, or utilized related to the College's organizational or institutional functions, students, employees, or constituents) will be assigned one of four data classification levels based on compliance, privacy, sensitivity, operational usage, and risk. Institutional Data must be protected with security controls and access authorization mechanisms identified within the College's InfoSec Program Regulation. The level of protection required for Institutional Data is based on the data classification level assigned to such data. Institutional Data includes, but is not limited to, information in paper, electronic, audio, and visual formats.

1. Applicability and Purpose

This Regulation applies to all College facilities, data, technology, faculty, staff, contractors, students, volunteers, visitors, sponsored guests of academic and administrative units, affiliated entities, and third-party service providers who have access to the College's Institutional Data. The purpose of this Regulation is to protect the College's Institutional Data while preserving the open, information-sharing mission of its academic culture. The College classifies Institutional Data in accordance with

legal, regulatory, administrative, and contractual requirements; intellectual property and ethical considerations; strategic or proprietary value; and/or operational use.

2. Data Classification and Permitted Use

The following rules and definitions delineate types of data and provide instructions for usage of that data. Based on the data classification level, authorization to access Institutional Data will vary and specific controls for access and protection will be applied in accordance with College's InfoSec Program Regulation. Proper classification is a prerequisite to enable compliance with legal and regulatory requirements, as well as institutional Compliance Measures. Compliance Measures are defined in Regulation 4.7002AR as *authoritative*, *semi-authoritative*, or *prescriptive/non-authoritative* documents in the InfoSec Program which address a specific area or category of information security and define the appropriate security requirements for that area or category. The four Institutional Data classifications are, from most to least restrictive:

2.1 ***Class 1: Restricted and Sensitive, High Risk.*** Class 1 data is Institutional Data that requires the highest level of protection and monitoring due to legal, regulatory, administrative, contractual, rule, or policy requirements. Access to and management of restricted data is strictly limited as unauthorized use or disclosure could substantially or materially impact the College's mission, operations, reputation, finances, or result in potential identity theft. Additionally, data and systems are categorized as Class 1 when the following risk factors are present. If:

- Protection of the data is required by law/regulation,
- The College is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or
- The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on the College's mission, safety, finances, or reputation.

2.2 ***Class 2: Private and Confidential, High Risk.*** Class 2 data is Institutional Data classified as private due to legal, regulatory, administrative, or contractual requirements; intellectual property or ethical considerations; strategic or proprietary value; and/or other special governance of such data. Access to and management of private data requires authorization and is only granted to those data users as permitted under applicable law, regulation, contract, rule, policy, and/or role. The data and systems are categorized as Class 2 when the risk factors itemized under the Class 1 heading are present, but the data is not designated by the College to be restricted or sensitive.

2.3 ***Class 3: Internal, Moderate Risk.*** Class 3 data is Institutional Data used to conduct College business and operations. It may only be accessed and managed by data users whose role, function, or assignment requires it. Unless otherwise indicated, internal is the default level for Institutional Data. Additionally, data and systems are categorized as Class 3 when the following risk factors are present. If:

- The data is not generally available to the public, or
- The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on the College's mission, safety, finances, or reputation.

2.4 ***Class 4: Public, Low Risk.*** Class 4 data is Institutional Data that is intended for public use and has no access or management restrictions. Additionally, data and

systems are categorized as Class 4 when their risk factors are defined as shown below. If:

- The data is intended for public disclosure, or,
- The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on the College's mission, safety, finances, or reputation.

2.5 ***Data Categorization and Permitted Use.*** The College's Institutional Data element categorization process will be accomplished by means of specific delegated department and team assignments for the above listed data classifications. Their permitted use in core College services and data user activities will be specified and itemized during the creation of the following mandatory reference documents

- **Institutional Data Element Classification Assignments.** Maps Institutional Data elements to the appropriate data classification levels.
- **Permitted Data Usage By Activity.** Identifies which classifications of Institutional Data are permitted for specific data user activities.
- **Permitted Data Usage By Service.** Identifies which classifications of Institutional Data are permitted for specific core or hosted services.

3. Review Cycle

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

4. 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 InfoSec Compliance Measure, the College's first recourse will be to promptly notify and offer corrective training to the offender. 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 termination of employment, student suspension or 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 the College's Senior Leadership Team stakeholders.

Every College Associate Vice President, Dean, and Director, alongside College-designated Risk Owners (as defined in the InfoSec Program Regulation 4.7002R, Section 8.3), is responsible for implementing and ensuring compliance with the College's InfoSec Program and must initiate corrective action through proper channels at the College if it is warranted. Responsibilities include:

- Applying the InfoSec Program's data classifications, mandates, and guidelines for Institutional Data resources to the Institutional Data under their stewardship.
- Communicating this Regulation to employees.
- Establishing specific goals, objectives, and action plans to implement this regulation.
- Developing plans that guide information system and database usage to satisfy institutional information needs.
- Actively supporting strong data management through data stewardship.
- Ensuring availability of education and training in data management principles, including security awareness, to individuals who access, maintain, or use this data.
- Providing an appropriate level of security that corresponds to the classification of the information.

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