BROOKDALE COMMUNITY COLLEGE
COLLEGE REGULATION

4.7002R Information Security Program Regulation

I. Title of Regulation

Information Security Program Regulation

II. Objective of Regulation

To authorize and establish rules, procedures, and standards to govern Brookdale Community College's ("the College") information security program ("the InfoSec Program"). The InfoSec Program Regulation is designed to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the College, the nature and scope of the College's activities, and the sensitivity of any of the College's information at issue. The InfoSec Program is purposefully intended to protect the College's data and information, any loss of which may represent a threat to the well-being of the College, the College community, Persons, or Third Parties.

III. Authority

President, Board of Trustees Policy 4.7002 Information Security Program

IV. Regulation Statement

Security breaches of data and technology pose a very real and very expensive threat to the College. Security safeguards must be in place to protect the College from these threats, based upon the risk they impose. The purpose of this Regulation is to enable the College to help protect all College data and technology. This Regulation will help the College implement, maintain, and continually improve its InfoSec Program.

1. Applicability

This Regulation includes information security management for all College facilities, data, technology, faculty, staff, contractors, students, and third-party service providers.

2. Introduction

Information is a resource of great value to the College as are information systems, resources and processes that facilitate creation, collection, use, sharing, or storage of information over the course of operations at the College. It is therefore important to adequately preserve the confidentiality, integrity and availability of these important resources that the College relies upon to achieve strategic and operational objectives.

Information Security is the ongoing process of identifying, evaluating, and treating risks to the confidentiality, integrity, and availability of information, information systems, and other business information processing resources and activities (collectively known as "Information Assets") at

the College. The College will ensure the confidentiality, integrity, and availability of technology and data through the development and implementation of compliance measures that address various information security requirements. These standards will follow industry-defined best practices in securing technology and data.

The College is committed to implementing and continually improving Information Security controls, policies, and practices that:

- Provide clear responsibilities for Information Security across the College;
- Implement safeguards to manage risk factors and to help mitigate, transfer, or avoid risks that may adversely impact the confidentiality, integrity, and availability of Information Assets;
- Comply with applicable law, regulatory and industry requirements, and contractual obligations; and
- Provide assurance to College stakeholders that Information Security risks are responsibly managed.

The above objectives for Information Security will be primarily achieved through approval and implementation of the InfoSec Program.

3. Key Definitions

3.1 A ***Compliance Measure*** is an authoritative, semi-authoritative, or prescriptive/non-authoritative document in the Information Security Program which addresses a specific area or category of information security and defines the appropriate security requirements for that area or category.

3.1.1 An ***Information Security Regulation, Standard, or Control*** ("Regulation," "Standard," or "Control") is an authoritative Compliance Measure in the Information Security Program.

3.1.2 An ***Information Security Process or Procedure*** ("Process" or "Procedure") is a semi-authoritative Compliance Measure in the Information Security Program.

3.1.3 An ***Information Security Guideline*** ("Guideline") is a prescriptive/non-authoritative Compliance Measure in the Information Security Program.

3.2 ***Information*** refers to a body of knowledge, collection of information, or data obtained, produced, organized, shared, or managed by the College or authorized Third Parties over the course of its business operations. Information may be shared or stored in a physical or electronic manner, or may take the form of the spoken word. Information includes, but is not limited to, any document, record, file, data, data set, or definable unit of information from any source that is created, processed, shared, or stored by the College or authorized Third Parties in any manner. Information is not easily replaced without funding, skill, knowledge, resources, time, or any combination of these factors. Therefore, Information is considered a critical resource from the standpoint that it is used to build knowledge, accomplish business objectives, and sustain or create organizational value.

3.3 *Information Asset* refers to Information, Information Systems, wholly-owned or leased facilities, and other resources or activities related to processing or storage of Information. The value of an Information Asset is determined not only by its financial value, but also the impact it has in supporting organizational activities and achieving business objectives.

3.4 *Information Systems* refers to wholly-owned or leased computing hardware, software, and media components for collecting, processing, storing, or delivering Information, or performing operational tasks that involve Information.

3.5 *Information Security (or "InfoSec")* refers to the ongoing process of identifying, evaluating, and treating risks to the confidentiality, integrity, and availability of Information Assets.

3.6 *Information Security Program (or "InfoSec Program" or "Program")* refers to the Information Security objectives, requirements, controls, and processes prescribed in this Regulation as well as its framework of supporting standards, procedures, and guidelines.

3.7 *Persons* refers to all College employees, students, and stakeholders.

3.8 *Risk Owners* are those individuals responsible for identifying and managing risk factors that may adversely impact the confidentiality, integrity, and availability of Information Assets within their business function or span of organizational control.

3.9 *Third-Party Service Providers (or "Third Parties")* are entities with whom the College enters into a Third- Party agreement. Third Parties include employees, contractors, agents, and subcontractors of Third Parties who have access to, store, or process Information. Third Parties may also have access to, or may manage, Information Systems.

4. Roles and Responsibilities

The Board of Trustees delegates responsibility for the evaluation and approval of Compliance Measures that are part of the InfoSec Program to the College President.

The College's Chief Financial Officer (CFO) and Chief Information Officer (CIO) will serve as the College's InfoSec Officers. In this role, the CFO and CIO are responsible for the development, implementation, and continued administration of the Program's Regulations and Compliance Measures. Once approved by the President, the Regulations and Compliance Measures will be implemented by the CFO and CIO utilizing the College's Information Technology (IT) Governance structure.

Everyone at the College – full-time and part-time employees, students, and Third Parties – is responsible for supporting and complying with InfoSec Program requirements outlined in this Regulation. However, the following roles and responsibilities shall be specifically defined to implement and manage the InfoSec Program across the College:

4.1 *The College's Senior Leadership Team* shall be responsible for:

- Implementing and regularly improving the InfoSec Program so as to be compatible with organizational strategy and operational objectives;

- Providing adequate resources, and appropriately integrating the InfoSec Program across the College's business units and organizational processes;
- Promoting and supporting the InfoSec Program by communicating with relevant stakeholders the importance of achieving and complying with InfoSec Program objectives and requirements;
- Allocating budgetary resources for management, oversight, and continuous improvement of the InfoSec Program; and
- Providing direction and support to the CFO and CIO, as necessary.

4.2 The ***Chief Financial Officer (CFO), Chief Information Officer (CIO), and the College's IT Governance*** shall direct and manage implementation and continuous improvement of the InfoSec Program, including:

- Establishment of a process for identifying objectives for, and governance of, the InfoSec Program that is scoped across relevant business units, departments, and organizational processes;
- Maintenance of this Regulation and its supporting framework of Regulations, Standards, Controls, Processes, Procedures, and Guidelines;
- Design and implementation of an InfoSec risk assessment process that identifies and evaluates InfoSec risks against relevant risk criteria;
- Design and implementation of an InfoSec risk treatment process to drive formulation, implementation, and monitoring of InfoSec risk treatment plans by relevant Risk Owners;
- Reporting on the performance and effectiveness of the InfoSec Program to the College's Senior Leadership Team for review at regular intervals;
- Providing for employee awareness and necessary competence to understand the implications of not complying with InfoSec Program requirements and contributing to InfoSec Program effectiveness; and
- Monitoring and reporting on performance and effectiveness of the InfoSec Program to relevant College stakeholders.

4.3 ***Risk Owners*** are responsible for allocating or managing resources to address risk factors identified by the CFO, the CIO, and IT Governance or other relevant InfoSec Program stakeholders that may adversely impact the confidentiality, integrity, and availability of Information Assets within their business function or span of organizational control.

5. Segregation of Duties

Conflicting or overlapping InfoSec compliance responsibilities shall be segregated to confirm that consistent InfoSec governance and risk management is implemented across the College. Segregation of duties shall be defined based on risk factors determined and evaluated by IT Governance.

6. InfoSec Principles

All components of the InfoSec Program and requirements of this Regulation focus on addressing risks to Information Assets. Risks to Information Assets shall be evaluated and managed according to the following fundamental security criteria, or principles:

- ***Confidentiality*** – Information Assets may have varying levels of sensitivity and therefore need to be protected from unauthorized access or exposure. By adhering to the principle of Confidentiality, the College makes Information Assets accessible to only those individuals or processes with a legitimate need and who are authorized to access them.
- ***Integrity*** – Information Assets are relied upon to deliver value to students, staff, faculty, and stakeholders or make business decisions. By adhering to the principle of Integrity, the College develops and maintains Information Assets to meet business objectives using methods that provide for accuracy and completeness.
- ***Availability*** – Information Assets are expected to be accessible when needed to support business objectives. Adhering to the principle of Availability maintains access to Information Assets in a reliable and prompt fashion.

7. InfoSec Risk Management Framework

The College shall define and implement a framework for identification and management of InfoSec risks across the College. The Framework shall consist of the following components:

- A risk assessment process that is applied to identify, evaluate, remedy, and report InfoSec risks to applicable Risk Owners and the College's Senior Leadership Team;
- Procedures and implementation standards that outline mandatory InfoSec control categories, objectives, and requirements that must be achieved across the College;
- An awareness program to make College employees and relevant external parties aware of InfoSec compliance Regulations, Standards, Controls, Processes, Procedures, Guidelines, and expected practices as well as the implications of non-compliance;
- A management process to oversee the performance and evaluate the effectiveness of the InfoSec Program across the College at regular intervals.

8. Regulation Objectives and Compliance Measure Categories Overview

The objectives categorized and summarized below shall be established and relevant InfoSec compliance Regulations, Standards, Controls, Processes, Procedures, Guidelines, and practices shall be implemented and monitored to manage InfoSec risks across the College. To accomplish this, Compliance Measures and Compliance Measure categories will be added, removed, and modified depending on changes to best practices in the industry. Implemented Compliance Measures will require members of the College community to take steps to protect the College's data and technology and will be established in relation to one or more of the following categories:

8.1 *InfoSec Regulation*

This InfoSec Regulation defines the College's Senior Leadership Team's objectives and support for InfoSec. This Regulation shall be:

- Approved by the College's Senior Leadership Team, and subsequently published and communicated to employees and Third Parties, as applicable; and
- Reviewed annually or at more frequent intervals if significant changes to the scope of the InfoSec Program or the business of the College have occurred to evaluate the Regulation's suitability, adequacy, and effectiveness.

8.2 *Personnel Security*

Controls associated with Personnel Security shall be implemented to confirm that College employees and Third Parties understand and fulfill their InfoSec responsibilities. Personnel Security includes the following control objectives:

- Communication to, and agreement by, employees and Third Parties on their InfoSec responsibilities prior to employment or prior to providing services to the College, including requirements for confidentiality and non-disclosure of Information;
- InfoSec awareness, education, or training of employees and relevant Third Parties;
- Management responsibilities to confirm that employees and Third Parties understand and perform their duties in accordance with InfoSec Regulations and Compliance Measures;
- A disciplinary process to sanction employees or Third Parties for failure to comply with InfoSec Regulations and relevant Compliance Measures; and
- A process for employee termination and Third Party off-boarding to manage revocation of access to, and recovery of, Information Assets.

8.3 *Information Asset Management*

Information Asset Management controls shall be implemented to identify, classify, and assign responsibilities for protecting Information Assets, as practicable. Information Asset Management includes the following objectives:

- Identifying and maintaining an inventory of Information Assets and the Risk Owners responsible for their protection;
- Classifying Information Assets in a manner consistent with their value or business criticality; and
- Defined acceptable use, management, transfer, storage and disposal practices associated with Information Assets in accordance with an information classification scheme.

8.4 *Access Control*

The objective of Access Control is to restrict access to Information Assets or access to Information Systems. Only employees and Third Parties with a legitimate business need and who have been authorized by the College shall have access to Information Assets or Information Systems. Access Control shall be achieved through implementation of the following:

- Processes or procedures for managing employee and Third-Party access to Information or Information Systems that include access provisioning, review of access rights at regular intervals, and modification or termination of access rights;
- Controls and mechanisms to authenticate employee and Third-Party access to Information Assets or Information Systems; and
- Controls to monitor and prevent unauthorized access to Information and Information Systems.

8.5 *Physical & Environmental Security*

Physical and Environmental Security controls shall be implemented to prevent unauthorized physical access, damage, loss, theft, or disruption to tangible Information Assets, including College office locations or facilities. Physical and Environmental Security objectives shall be achieved through implementation of the following:

- Maintaining appropriate physical and environmental security controls, including entry controls, to safeguard restricted-access office locations and facilities;
- Protecting supporting utilities and computer equipment from environmental threats, power failures, or other disruption, based on applicable risk factors;
- Protecting computer equipment and other tangible Information Assets from theft or unauthorized removal; and
- Processes to dispose of computer equipment or other tangible Information Assets to securely remove Information prior to re-use or destroyed prior to final disposition.

8.6 *Network and Systems Infrastructure Security*

Network and System Infrastructure Security controls shall be implemented to protect and provide for the confidentiality, integrity, and availability of Information and Information Systems. Network and Systems Infrastructure Security controls shall include:

- Maintaining adequate documentation related to the design and operational performance of Information Systems;
- Maintaining a change management process to control planned and unplanned changes to Information Systems;
- Physical and/or logical separation of Information System development, test, and production environments, or applicable controls to safeguard the use of Information in development, test, and production environments;
- Security measures to detect threats, safeguard computing services, protect Information, or control access or changes to Information Systems;
- Protecting against Information loss by backing up Information and Information Systems and testing backups at regular intervals to allow the College to recover Information and Information Systems in timeframes sufficient to meet business requirements;
- Identifying and preventing against exploitation of technical vulnerabilities;
- Protecting against malware threats by employing solutions or processes to detect and recover from malware-based attacks; and
- Monitoring Information Systems to record and regularly review security events to identify unintended or unauthorized activity.

8.7 *Communications Security*

Communications Security controls shall be implemented to provide for the security of electronic communications networks and to protect Information. Communications Security shall be achieved through implementation of the following controls:

- Network segregation achieved by grouping Information Systems on segmented networks according to inherent risk factors;
- Controlling access between users and Information Systems on segmented networks;
- Appropriately securing communications to achieve acceptable levels of risk;
- Deploying mechanisms for network security monitoring according to inherent risk factors; and
- Maintaining requirements for secure exchange and storage of electronic Information, including the use of encryption.

8.8 *Applications Data Security*

Applications Data Security controls are associated with integrating InfoSec requirements across the entire Information lifecycle. Applications Data Security controls in this category shall include:

- Maintaining adequate documentation related to the operation and usage of applications or Information Systems;
- Maintaining an appropriate change management process to control planned and unplanned changes to applications or Information Systems;
- Analysis of InfoSec requirements for modifications to existing or new applications or Information Systems;
- Appropriately securing software and applications to achieve acceptable levels of risk;
- Security review and testing of Information Systems, including review and testing of software and applications; and
- Using carefully selected and protected data during software integration and quality assurance activities.

8.9 *Third-Party Security*

Controls shall be implemented to protect Information Assets that are shared with, accessible to, or stored by Third Parties. Security controls shall include:

- The stipulation that all Third-Party service providers shall be required by contract to implement and maintain InfoSec safeguards;
- A process to identify risks to Information Assets and incorporate InfoSec and relevant risk treatment requirements into business agreements with Third Parties; and
- Processes to monitor Third-Party performance towards InfoSec requirements.

8.10 *InfoSec Incident Management and Ongoing Risk Assessment*

Controls shall be implemented to provide for consistent and effective management of InfoSec incidents. InfoSec Incident Management and Ongoing Risk Assessment controls shall include:

- A defined process for InfoSec incident management that includes specific and delegated responsibilities, requirements for reporting potential security incidents by staff, incident assessment or classification criteria, and documented response guidelines;
- Communication to and awareness by relevant individuals of their role in the InfoSec incident management process;

- A defined process to capture and apply knowledge gained from InfoSec incidents to address and reduce the impact or likelihood of future occurrences;
- Ongoing effort to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of College information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks; and
- The evaluation and adjustment of the College's InfoSec Program in light of the results of such testing and monitoring.

8.11 *Business Continuity Management*

Controls shall be implemented to provide continued confidentiality, integrity, and availability of Information Assets, as well as to provide for the continuity of applicable InfoSec controls or processes, during unplanned, adverse events. Business Continuity Management controls include:

- A process to scope, document, and enact requirements for continuity of access to, availability, or recovery of, College Information Assets; and
- A process implemented at regular intervals to evaluate the effectiveness of business continuity activities.

8.12 *Compliance & Audit*

Compliance and Audit objectives are associated with the need to monitor business, legal, regulatory, or contractual requirements and confirm that InfoSec controls and requirements are implemented consistently. Such security controls shall include:

- Monitoring, identification and review of applicable legal, regulatory, or contractual requirements as they relate to InfoSec, including security and privacy of personal information; and
- Auditing compliance with InfoSec compliance regulations, standards, controls, processes, procedures, guidelines, or other requirements at regular intervals.

9. *Review Cycle*

This Regulation shall be reviewed annually by the Chief Financial Officer (CFO) and Chief Information Officer (CIO).

10. *Compliance and Enforcement*

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.

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

V. Responsibility for Implementation

Chief Financial Officer and Chief Information Officer

Approved: President, 8/22/2019