BUTLER COUNTY COMMUNITY COLLEGE

Information Security Policy

Purpose

Butler County Community College (BC3) has adopted the following Information Security Policy ("Policy") as a measure to protect the Confidentiality, Integrity and Availability of Institutional Data, as well as any Information Systems that store, process or transmit Institutional Data, and to comply with Laws and Regulations governing data privacy and protection.

Scope

This policy applies to all BC3 Employees, College Affiliates, and Students. It is critical everyone associated with providing or using Institutional Data or Information Systems is diligent when they safeguard data and respond to Security Threats to the Information Systems.

Policy

BC3 will ensure the Confidentiality, Integrity, Security, and Availability of Institutional Data as well as Information Systems through the development and implementation of Standards, Procedures, and/or Guidelines that follow industry-defined best practices.

Roles and Responsibilities

The Director of Information Technology in conjunction with the Dean of Admissions and College Registrar, and/or the Executive Director of Human Resources/Equal Opportunity Compliance Officer is responsible for the enforcement of this Policy.

All BC3 Employees, College Affiliates, and Students play a critical role in ensuring the success of the Information Security Policy. Everyone has the responsibility to protect information resources and report any suspected information security incidents to the appropriate manager and the Director of Information Technology. That responsibility **must be** viewed as a top priority.

Enforcement

Violations of this Policy and related Standards, Procedures, and Guidelines may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and BC3 owned Information Systems; BC3 reserves the right to take disciplinary action, up to and including termination of employment, permanent student dismissal, and/or legal action.

Definitions

Availability
The assurance that information and communications services will be ready for utilization when expected

BC3 Employees
Any persons employed by the College including, but not limited to, faculty, staff, administrators, and student workers

College Affiliates
Any persons doing business for or on behalf of BC3 such as volunteers, interns, contractors, consultants, vendors and other individuals working under agreements with the College

Confidentiality
Ensures that data is kept private and\or an Information System is accessed by only an authorized person

Guidelines
Recommendations designed to streamline certain processes according to best practices

Information System
Any electronic system that stores, processes, or transmits information

Integrity
The assurance that the data or Information System can be trusted. Ensures that it is edited by only authorized persons and remains at its original state when at rest

Institutional Data
Any data (paper, digital, or other electronic media) that is owned, stored, or licensed by BC3

Laws and Regulations
A system of rules created and enforced through social or governmental institutions including, but not limited to, FERPA, NIST, HIPPA, Gramm-Leach Bliley, Clery Act, PCI-DSS, and GDPR

Procedures
Detailed step-by-step instructions to achieve a given goal or mandate

Safeguard
A measure taken to protect the security of an asset

Security Threat
A malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization

Standards
Mandatory courses of action or rules that give formal policies support and direction

Student
Anyone that has applied for and taken any credit courses or non-credit classes/training at BC3

Board Approved 5/18/2022