INFORMATION SECURITY PROGRAM Effective December 15, 2021
Procedure 15-02 (B)

(1) PURPOSE

(a) The Program complies with applicable federal and state laws and regulations on the protection of Personal Identifiable Information (PII) and Nonpublic Financial Information (NFI) found in records and in computing resources maintained by the College and College employees. The Program also aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Columbus State takes measures to safeguard confidential College information and provides notice about security breaches of protected College information to affected individuals and appropriate agencies.

(b) The College also operates and maintains a computer security incident response plan that detects and reacts to computer security incidents, determines the scope and level of risk, remediates risk, communicates risk and results to stakeholders as well as reduces the likelihood of reoccurrence.

(2) GOVERNANCE

(a) The Administrator of Information Security or designee is responsible for maintaining, implementing, reviewing and updating the Program.

(b) The Program establishes an Information Security Committee (Committee) comprised of members of the College community who review the Program and make recommendations for improvement to ensure the appropriate standards, processes and guidelines are in place. The Committee also promotes training and communication to raise awareness of the importance of protecting information.

(3) REPORTING ATTEMPTS AND ACTUAL BREACHES OF DATA

All incidents of potential or actual unauthorized access to or disclosure, misuse, alteration, destruction or other compromise of information, or of a breach or attempted breach of information, must be reported immediately to the IT Support Center.

(4) RISK ASSESSMENT

(a) Columbus State continuously evaluates reasonably foreseeable internal and external risks to all College information. To the extent technologically and operationally feasible, Columbus State seeks to identify paper, electronic and computing resources containing College information. These evaluations are performed in the normal course of business and in cooperation with departments across the College. Recommendations arising from these efforts are made to the appropriate areas for consideration and implementation.

(b) Columbus State continuously evaluates reasonably foreseeable internal and external risks to all forms of information. These evaluations are performed in the normal course of business and in cooperation with departments across the College. Recommendations arising from these efforts are made to the appropriate areas for consideration and implementation.

(5) COMPLIANCE

(a) Each authorized user of computing resources is responsible for compliance with all applicable laws, College policies and applicable restrictions, whether or not the restrictions are built into the computing resource and whether or not they can be circumvented by technical means.

(b) College departments and IT staff will monitor compliance with the Program during the normal course of business.

(6) VIOLATIONS

Users who access, disclose, misuse, alter, destroy or otherwise compromise information without authorization or fail to comply with the Program may be subject to legal action and/or sanctions or disciplinary action.

(7) CONTROLS

(a) Columbus State maintains administrative, technical and physical controls to protect College records.

(b) An Information Security Standards Guide related to the Program is published and maintained separately within IT.

(8) THIRD-PARTY VENDOR RELATIONSHIPS

Columbus State exercises appropriate due diligence in selecting service providers to determine the capability of maintaining appropriate safeguards for College information. All contracts with third parties accessing or connecting to College computing resources are reviewed and approved by IT.

(9) TRAINING

The College provides different information security awareness trainings. Some training (i.e. HIPAA, PCI and FERPA) may be required based on job duties.

(10) The following Columbus State program and policies provide advice and guidance related to this procedure:

(a) Identity Theft Prevention Program (Red Flag Rule)

(b) College Policy 7-05, *Student Records*

(c) College Policy 9-12, *Payment Card Industry Compliance*

(d) College Policy 11-04, *Records Retention and Disposal*

(e) College Policy 15-01, *Responsible Acquisition and Use of Computing Resources*

New Procedure