Allegany College of Maryland

TECHNOLOGY SECURITY POLICY

Adopted date 6/18/2018
Revised Date 6/17/2022
Approved by Board of Trustees 6/18/2022
Implementation 6/18/2022
Type of Policy: Operational

BACKGROUND AND PURPOSE

Allegany College of Maryland acknowledges its obligation to ensure appropriate security for Information and systems that are considered vital assets to our organization. The College also recognizes its responsibility to promote security awareness among faculty, staff and students. Therefore, it is crucial for the College to establish a fundamental framework to ensure the protection of its information from unauthorized access, modification, disclosure, and destruction.

This policy describes Allegany College of Maryland's (ACM) safeguards to protect the confidentiality, integrity, and availability of information and information technology resources. This policy is following the provisions of the Gramm-Leach-Bliley Act of 2002 regarding the Safeguards Rule of customer records, the FTC Red Flags Rule of 2008, the privacy rules of the Family Educational Rights and Privacy Act (FERPA) of 1974, The Health Insurance Portability and Accountability Act of 1996 (HIPAA), European Union General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).

POLICY

I. SCOPE OF THE POLICY

This policy applies to all College information that is electronically generated, received, stored, typed, copied, and printed. The provisions of this policy apply to activities, methodologies, and procedures implemented by institutional departments, units and the Information Technology Department to protect all College data.

II. POLICY STATEMENT

It is the plan of Allegany College of Maryland to implement and maintain an information security strategy that provides a robust, adaptable and defensible security posture to address current and future needs and threats. The College's administration will keep guidelines for the design, implementation and maintenance of procedures for protecting the computer and data assets of the College. These guidelines will be updated as needed to meet the compliance requirements set forth in federal, state and Institutional rules, standards, laws and regulations. The following procedures will define the basis for our security guidelines:

- Access Control
  - Separation of User and Administrative Functions
  - Account, Password and Multi-factor Authentication Management
- System Operation and Administration
  - System Standards and Documentation
  - Risk Management Process
  - Disaster Recovery Planning
  - Incident Response Process
- Security Management
  - Data and System Classification and Protection
  - Datacenter Physical and Environmental Protection
  - Backup, Recovery, Archiving and Data Disposal
  - Wired and Wireless Network Protection
  - Vulnerability Monitoring, Reporting, Patching, Review and Testing
  - Employee Security Awareness Training
- Information System Acquisition, Implementation and Maintenance
- Change Control Management

III. Responsibility

Every member of the College community is responsible for protecting the security of information and information systems by adhering to all related policies, standards and guidelines such as, never storing College information on a personal device.

IV. Enforcement

Users found to have violated this policy may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Any corrective measures taken shall be administrated in accordance with appropriate disciplinary procedures applicable to the relevant user.

V. Related Policies and Standards

Technology Security Standard, Mobile Device Standard, Breach Notification Policy, Breach Reporting Procedures, Technology Resources Policy.

VI. Administration of Policy

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining this policy.

VII. Changes

Substantive changes to this policy require approval by the Board of Trustees; editorial changes, title/position changes, and/or changes to its implementation procedures may be made as required by federal or state mandate and/or institutional need with timely notice to students and employees.