Allegany College of Maryland
Technology Security Policy

Issued: 7/18/2017 **Approved**: 6/18/2018

Purpose

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 in compliance with 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).

Scope

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 information.

Introduction

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.

Policy

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
- System Operation and Administration
    - System Standards and Documentation
    - Risk Management Process
    - Disaster Recovery Planning
    - Incident Response Process
    - Security Awareness Training
- Security Management

  - System Classification and Protection
  - Data Classification and Protection
  - Datacenter Physical and Environmental Protection
  - Backup, Recovery, Archiving and Data Disposal
  - Network Protection
  - Vulnerability Review and Testing
  - Monitoring and Reporting
- Information System Acquisition, Development and Maintenance
- Change Control Management

Responsibility

Every member of the College community is responsible for protecting the security of information and information systems by adhering to all related policies and guidelines.

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.

Related Policies/Standards:

Technology Security Standard, Breach Notification Policy, Breach Reporting Procedures

Revision History

Version Number	Date	Author	Description
1.0	3/27/2017	Rich Crawford	Initial Draft
1.2	7/18/2017	Rich Crawford	Revised Draft
1.3	3/19/2018	Rich Crawford	Revised Draft
2.0	5/8/2018	Rich Crawford	IT Governance Committee Approved
2.2	5/16/2018	Rich Crawford	President’s Advisory Team reviewed
2.3	6/18/2018	Rich Crawford	Board of Trustee’s approved