Allegany College of Maryland

TECHNOLOGY SECURITY STANDARD

Adopted date 6/18/2018
Revised Date 6/17/2022
Reviewed by Board of Trustees 6/18/2018
Implementation 6/18/2018
Type of Standard: 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. Therefore, it is crucial for the College to establish and maintain appropriate security procedures to ensure the protection of its information from unauthorized access, modification, disclosure, and destruction.

The purpose of this standard is to define appropriate security measures, administrative direction, procedural requirements, and technical guidance that must be implemented to *protect* the data and resources residing at Allegany College of Maryland.

STANDARD

I. SCOPE OF THE STANDARD

The scope of this standard specifically focuses on the following areas:

- Risk Management Process
- IT Incident Response Process
- IT Disaster Recovery Plan
- Security Awareness

II. STANDARD STATEMENT

This information security standard prescribes a set of minimum-security requirements necessary to protect the confidentiality, integrity, and availability of information. Allegany College of Maryland (ACM), as a trusted entity, will carry-out those security requirements in accordance with federal and state laws, directives, policies, regulations, standards and guidance. Thus, all information generated, received, stored, typed, copied, and printed with ACM's resources for the purpose of conducting college-related business is protected under the provisions of this Technology Security Standard.

III. Risk management process

Allegany College of Maryland (ACM) performs risk assessments on critical IT systems. This task is performed by the System Administrators and the Security specialists during system implementation, scheduled replacement, and update cycles. Also, risk assessment is performed by the external auditors. The College recognizes that the risk of unauthorized use of information or access to information is probable. These risks include but are not limited to:

- Unauthorized access of information by an individual not considered the information owner.
- Compromised system security due to system access by an unauthorized individual.
- Interception of data during transmission.
- Loss of data integrity.
- Physical loss of data in a disaster.
- Errors introduced into the system.
- Corruption of data or systems.
- Unauthorized access of information by employees.
- Unauthorized requests for information.
- Unauthorized access through paper (hardcopy) documents.
- Unauthorized transfer of information through a third-party.

ACM acknowledges that the above list of potential risks associated with the protection of information is not exhaustive. Notably, new risks of unauthorized use or access to information are created regularly due to the rapid

advances in technology. However, the Information Technology Department will actively participate and monitor advisory groups such as US-Cert, the Educause/Internet2 Security Working Group, (SANS) Institute for identification of new risks to safeguard the college's information, and the National Institute of Standards (NIST) Computer Security Resource Center.

IV. Administrative Safeguards

Access to information from any of Allegany College of Maryland's computer information systems is limited to employees who have a legitimate business reason to such information. Databases containing personal and sensitive information including but not limited to, students' accounts, balances, grades, financial records, employees' records and confidential information are available only to ACM's employees in appropriate departments and positions. Each employee is given an account and password after documentation from the Human Resources Department (HR) has been received by the Information Technology Department.

After a completing the application process for admission to the College each student is given an account with access to their email, course information and Learning Management System via the College's credentials creation process. Student access is restricted from any information system or information technical resource that is considered "Administrative." The Information Technology Department will continue to take appropriate measures that are consistent with existing technological developments to ensure that all College information is secure, and to safeguard the confidentiality, integrity, and vailability of information and information technology resources.

V. Operational Safeguards

The operational safeguards address security controls that are implemented on information systems. These controls help to enhance the security of the College's information and information technology resources. The controls are put in place by the professional staff in the Information Technology Department, and enforced through policy, standards and operating procedures.

VI. Access Controls

All "administrative" accounts require a valid user name and password in order to obtain access to any College information and information technology resource. To enhance security, these accounts will use Multi-factor Authentication (MFA) in addition to a standard username and password. The authentication (logon process) will not occur without the above requirements.

All users will adhere to the minimum acceptable Password Standard described below:

- Password History = 5
- Minimum Password Age = 5 days
- Maximum Password Age = 180 days
- Minimum Password Length = 9 characters
- Maximum Password Length= 16 characters
- Password Complexity = addition of 1 upper and lower case, 1 numeral and 1 special character
- Account Lockout standard = 3 failed attempts
- MFA will be used along with the standard username and password

In addition to the above-mentioned controls, access to critical systems is further enforced through the following standard operating procedures:

- The new user onboarding process originating from Human Resources
- User access entitlement review performed by supervisors
- Termination of user accounts originating from Human Resources

VII. Network Controls

Access to any network-connected computer must be via a logon process that identifies and authenticates the user, except where read-only access is given to a certain system, such as the library catalog, or unprivileged access is normal and the appropriate safeguard is in place, such as guest/public access in the Open Computer Labs. Also, computers configured with the whole or partial purpose of accepting connections from and exchanging information between other computers are defined by this standard as a server. The following controls apply to networked computers and servers:

- Servers must be located in secure areas with physical access controls such as keys, access cards, and or alarms. Unauthorized users who require physical access to a server, or require access in the vicinity of a server, must be escorted by an authorized systems administrator.
- Servers must be located in an area that has the appropriated environmental controls, including air handling and conditioning, uninterruptible power protection (UPS) and conditioning, and fire suppression.
- Servers must be appropriately managed and monitored on a daily basis by an authorized systems administrator.
- Only an authorized systems administrator may modify a computer's network settings and parameters.

VIII. Independent Network Controls

Independent Networks are systems connected to the college's IT infrastructure, but are not managed by the Information Technology Department. These networks include the Internet, AcademicWorks, Ellucian Cloud, OmniUpdate, Navigate, Parchment, Brightspace SaaS, Evolve-Elsevier (HESI exam), ACI ecommerce payment processing and Nelnet payment systems. The owners and users of independent networks are required to comply with the College's policies and standard operating procedures, including the safeguards described in this security standard. Some of the safeguards pertinent to this standard include, but are not limited to:

- All independent networks that have the capability to bypass the College's firewalls and ACLs must be approved and registered with the Information Technology Department prior to being connected to the College's network infrastructure. These independent networks include technologies associated with dialup access, wired access, wireless access, and Virtual Private Networks (VPNs).
- Network staff in the Information Technology Department shall configure firewalls and routers' Access Control Lists (ACLs) to restrict the types of traffic that may be allowed to enter and leave the College's network infrastructure.

All devices associated with independent networks shall be monitored and scanned to detect potential threats or a security breach. If a breach is perceived, System Administrators and Security Specialists will be notified immediately. In the event, these staff are unavailable a Network Administrator will disconnect that device(s) from the College's network infrastructure.

IX. Wireless Controls

The airwaves local to Allegany College of Maryland's campuses are considered a transmission medium, whereby voice and data communications are prevalent. As the airwaves are a shared resource, the Information Technology Department is responsible for the management and allocation of bandwidth in this medium. This process is administered through the use of Wireless Access Points (WAPs). WAPs refer to devices which serve as a connection between wireless and wired technologies. This includes all forms of wireless networking, such as hardware, software, and wireless telephones including Radio Frequency (RF) and Infra-Red (IR) devices. The following processes apply to the use of the College's airwaves for voice and data transport:

- All wireless access points must be pre-approved and registered by the Information Technology Department prior to being deployed for service.

- All wireless access points must be secured from unauthorized use. Appropriate forms of authentication and authorization will vary depending on the wireless medium.

X. Patch Controls

Reasonable attempts must be made to secure servers against published security vulnerabilities. This includes the timely application of patches, service packs, and hot fixes to operating systems and applications, as long as the corrective action itself will not adversely affect the proper operation of the server. The following controls apply to networked computers and servers:

- Critical operating system patches must be installed on all systems in 7 days of release
- Critical application patches must be installed on all systems in 30 days of release

XI. Antivirus Controls

All networked computers and servers must have anti-virus protection installed. The following controls apply:

- Anti-virus software must be installed on all systems
- The most recent version of anti-virus software must be maintained with current virus signature/patterns on all systems

XII. Backup and Recovery Controls

In an effort to preserve the College's information in the event of a partial or total loss of resources, the Information Technology Department applies the following controls to servers:

- The servers containing "critical" data are routinely backed up.
- Servers and network devices necessary to the continued operation of the College's technology services are maintained on a hardware support plan. This provides recovery from any hardware failure within 12 to 72 hours.
- Servers and network devices critical to the continued operation of the College's technology services are configured in fault-tolerant designs or utilizing on-site spares where ever possible.
- Data that has been backed up is tested periodically to ensure that the media and restoration procedures are functioning and that the data is actually retrievable.
- Full backups are stored at both onsite and offsite locations.

XIII. Software Controls

In accordance with the terms of software applications and compliance with copyright laws, the College exercises the following controls regarding the installation and use of software on all computing devices owned or leased by Allegany College of Maryland (ACM):

- All software that is installed on computing devices must be licensed through the College.
- Software installations must be performed by an authorized IT technician.
- Licensing information for standard software applications must be maintained by IT.
- The IT Department will perform licensing audits on standard software applications.

In addition to the above-mentioned software controls, the College enforces same through policies development (referenced in the Technology Resources Policy, Email Use Policy, Wireless Network Security Policy and Mobile Computing Devices Standard), including but not limited to:

- Software Use for Faculty and Staff
- Faculty and Staff Computer Use & Internet Access
- Student Computer Use & Internet Access
- Faculty and Staff Wireless Use
- Student Wireless Use

XIV. Incident Response

Allegany College of Maryland follows a systematic process for identifying, tracking, and responding to information security incidents. The coordination of all activities related to an IT Incident Response will aid in protecting the confidentiality, integrity, and availability of the College's information and information technology resources, as well as accelerate the remediation cycle. The College reserves the right to take necessary action under this standard to protect its resources and/or preserve evidence.

XV. IT Incident Response Process

In the event of an information security incident or breach, the College will undertake the necessary processes to remedy the incident or breach, in hopes of preserving the College's information and information technology resources in accordance with the Breach Notification Policy, Breach Reporting Procedures and the steps outlined herein.

XVI. IT Response Team

The Information Technology Department response team of IT professionals will assemble to address a breach or information security event or incident. The team consists of the:

- Dean of Information Technology
- Network/Security Engineer
- Datacenter Administrator
- Coordinator Database and System Design
- Coordinator of Technical Services
- Coordinator of Web Services
- System Programmer Analyst
- Helpdesk Coordinator
- Vice President of Finance and Administration (for reporting purposes)

XVII. Incident Classification

In this standard, an information security incident falls into one of two categories: A high severity incident and a low severity incident. The Dean of Information Technology or designee is responsible for escalating a reported event to an incident, and initiating an incident response, according to the classification described below.

A **high severity incident** involves unauthorized access to information, loss or theft of a device known to store, process, or transmit highly sensitive information. Also, a high severity incident includes, but is not limited to, a compromised networking device such as a router or switch, an unauthorized change in the configuration of a firewall, an intrusion detection system, the unavailability of a critical system needed to perform daily transactions, a widespread attack on critical and non-critical College systems or an infrastructure failure.

A **low severity incident** involves any information security incident that does not fall in the high severity classification.

XVIII. Initial Report and Assessment

The processes relevant to reporting and assessment specify actions required by Allegany College of Maryland's personnel reporting or responding to an information security event or incident that may threaten the confidentiality, integrity, and availability of the College's information and information technology resources.

These processes include but are not limited to:

- All members of the College are responsible for reporting known or suspected information security events promptly to the Help Desk via email or telephone:
    - Help Desk - IThelpdesk@allegany.edu or 301-784-5444
- The Help Desk staff person receiving the report will contact the appropriate personnel for the system. If the reported event appears to meet one or more high severity criteria described in the Classification section of this standard, the Help Desk staff person will contact the Dean of Information Technology or designee to evaluate the event.
- The Dean of Information Technology or designee is responsible for escalating a reported event to an incident and initiating an incident response. All incidents will follow the processes defined herein in accordance with the Breach Notification Policy and Procedures.
- All individuals involved in reporting or investigating an information security event or incident is obliged to maintain confidentiality, unless the Dean of Information Technology or designee authorizes information disclosure.
- Any exceptions to these processes must be approved by the Dean of Information Technology or designee.

XIX. Mitigation and Containment

Upon notification of a potential breach, a system administrator or network engineer shall take the necessary actions to immediately terminate unauthorized access by an intruder, eliminate the method of access used by the intruder, and eradicate any related vulnerabilities. Systems that have been infected with malicious code or systems accessed by an intruder shall be isolated from the network, until the extent of the damage can be assessed.

XX. Response and Investigation

All declared information security incidents will warrant a priority response from the Information Technology Department. The response will encompass protecting the College's information and information technology resources, containing any damage or spread, preserving evidence, eradicating damage, and restoring systems. Also, during the response and investigation phases, the Dean of Information Technology or designee will be responsible for communicating with other College personnel or officials for the purpose of update and instruction, for the duration of the incident. During the investigation of the incident, every effort shall be made to preserve log and system files that could be used as evidence of an information security incident. This may include backing up the affected system(s), documenting all activities performed on the affected system(s), storing drives and tapes in secured safes, and documenting and controlling the movement and handling of potential evidence in an effort to maintain a sense of guardianship. The IT staff involved in the response shall serve as the central point for collection of evidence. In conjunction with the investigation of an incident, the college will follow the business continuity plan defined in the College's disaster recovery plan so that critical business activities will not come to a halt, or if so, only for a minimum amount of time. However, business continuity will not take precedence over the activities necessary to contain damage or preserve evidence. Therefore, individual departments must be prepared to handle an interruption in service as a result of actions needed to contain and remedy the incident. Thus, all departments within the College are required to have a business continuity plan in place so that critical College business will not be discontinued during an unforeseen circumstance, including but not limited to, an information security incident.

XXI. Eradication and Restoration

The Information Technology Department will determine the extent of damage to the system(s) affected by the incident. If the damage is severe and the integrity of the information data is controversial, this may require that the system(s) be shut down and a complete restoration of the operating systems and data be initiated. The Dean of Information Technology or designee must notify the appropriate College officials if in fact a critical system must be taken off-line for an extended period of time in order to perform a system restoration.

XXII. Documentation and Final Report

Disseminating information to the appropriated personnel is an essential process in the response to an incident. If an incident extends beyond 4 hours, the individual directly involved in addressing the incident should provide the Dean of Information Technology and their immediate supervisor with updates on the status of the incident and the remediation efforts. The Information Technology Department is responsible for preparing documentation for the incident report. The actual report should be submitted by an individual directly involved in addressing the incident.
All information relevant to the incident must be written on the IT Incident Report and filed within three business days of the conclusion of the incident.

The incident report should include the following information:

- The name of the individual submitting the report.
- The affected system(s) and their respective location(s).
- A description of the system(s) including hardware, operating system, application software, and the function or purpose.
- A description of the information security incident.
- An assessment of the damage or loss.
- The status of the system in terms of incident resolution.
- The corrective action(s) taken to resolve damage or loss to the system(s).

The Information Technology Department shall manage the dissemination of incident information to College officials, including but not limited to the President, Vice Presidents and/or Department heads. Additionally, the College will comply with any reporting requirements imposed by state and federal laws. If the incident could affect the public or imposes user misconduct or criminal activities appropriate law enforcement agencies will be contacted. The dissemination of incident information either from the department or through the College shall be handled appropriately in exposure of sensitive information.

XXIII. Incident Prevention

The continuous development of processes for the configuration of the College's information and information technology resources is critical to the ongoing initiative of protecting the confidentiality, integrity, and availability of information. Therefore, Allegany College of Maryland will monitor, scan, and test its information technology infrastructure on a regular basis For anomalies to prevent information security incidents.

XXIV. Disaster Recovery Plan

Allegany College of Maryland's (ACM) IT systems are vital resources needed to conduct business processes. Notably, the College's success is dependent upon the services that these IT systems provide; thus, is crucial that these systems be operational without unnecessary interruption. To that end, the College has established an IT Disaster Recovery Plan outlining the procedures that facilitate an effective and expedient system recovery, subsequent to a service disruption or disaster. ACM's IT Disaster Recovery Plan is a comprehensive document that is
separate from this document.

XXV. Security Awareness

Allegany College of Maryland ensures that users understand their roles and responsibilities for information security through ongoing awareness. The focus on IT security concerns and how users should respond to those concerns are paramount to minimizing security events or incidents. Therefore, the College promotes awareness through existing policies and standard operating procedures. Also, the Information Technology Department presents awareness through email notifications such as security Alerts and Updates. Additionally, the department works in conjunction with the Human Resources Department to provide IT system information to new users during orientation. The College is committed to enhancing programs and services for all stakeholders and will evaluated and revised security awareness initiatives on an annual basis. Thus, there will be opportunities to implement more mechanisms to address security awareness effectively in the ACM community.

XXVI. Summary

This Technology Security Standard is enforced and supported by ACM's policies, standard operating procedures, and state and federal laws. Specifically, the standard identifies the necessary safeguards and processes to protect the College's information from unauthorized access, modification, disclosure, and destruction. All stakeholders, including but not limited to faculty, staff, students, alumni, board members, members of the community, vendors, contractors, affiliations, and partners are required to comply with these processes and controls documented in this standard, as well as, all other College policies and procedures. This standard shall be reviewed and updated once every two years.

XXVII. Enforcement

Users found to have violated this standard 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.

XXVIII. Related Policies and Standards

Technology Resources Policy, Wireless Network Security Policy, Breach Notification Policy, Breach Reporting Procedures

XXIX. 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.

XXX. 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.