Manhattan Area Technical College
Institutional Policy and Procedure Manual

Policy No. 9.1.7

Title: **GLBA Infomrmation Security Program Policy**	
Originated by: Chief Information Officer/Director of Facilities	Originated Date: 4/2023
Revised by:	Revised Date:
President/Board of Directors Approval Date:	
Reviewed on:	

Policy Statement: GLBA mandates that the Institute appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and Information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Rationale: This Information Security Plan describes Manhattan Area Technical College safeguards to protect covered data and Information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Billey Act (GLBA).

These safeguards are provided to:

- Ensure the security and confidentiality of covered data and Information.
- Protect against anticipated threats or hazards to the security or integrity of such Information.
- Protect against unauthorized access to or use of covered data and Information that could result in substantial harm or inconvenience to any student or employee.

This Information Security Program also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and Information maintained by MATC.
- Develop written policies and procedures to manage and control these risks.
- Implement and review the program.
- Adjust the program to reflect changes in technology, the sensitivity of covered data and Information, and internal or external threats to information security.

Procedure:

Information Security Program Coordinator(s)

The Chief Information Security Officer/Director of Facilities and the Network Administrator have been appointed program coordinators at MATC. They are responsible for assessing the risks associated with unauthorized transfers of covered data and Information and implementing procedures to minimize those risks to the college. They will also conduct reviews of areas that have access to protected data and Information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security policies and practices delineated in this program.

Identification and Assessment of Risks to Student/Employee Information

MATC recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and Information by someone other than the owner of the covered data and Information.
- Compromised system security as a result of system access by an unauthorized person.
- 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 covered data and Information by employees.
- Unauthorized requests for covered data and Information.
- Unauthorized access through hardcopy files or reports.
- Unauthorized transfer of covered data and Information through third parties.
-

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and Information and that new threats are created regularly, MATC will actively participate and monitor appropriate cybersecurity advisory groups to identify risks.

Current safeguards implemented, monitored, and maintained by MATC are reasonable, and considering current risk assessments are sufficient to provide security and confidentiality to the covered data and Information the Institute maintains. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such Information.

Employee Management and Training

Per MATC policies, standards, and guidelines, reference checking and background reviews are conducted for all new hires. During employee orientation, each new employee in departments that handle Protected Information are required to participate in several training sessions on the importance of confidentiality of Protected Information. Each new employee will also be trained to use computer information and passwords properly. Further, each department responsible for maintaining Protected Information will provide ongoing updates to respective staff. These training efforts should help minimize risk and safeguard covered data and information security.

Physical Security

Manhattan Area Technical College has addressed the physical security of Protected Information by limiting access to only employees with a business reason to know or access such Information.. Existing policies establish a procedure for promptly reporting the loss or

theft of Protected Information. Offices and storage facilities that maintain Protected Information limit customer access and are appropriately secured. Paper documents that contain Protected Information are shredded at the time of disposal.

Information Systems

Information systems include network and software design and information processing, storage, transmission, retrieval, and disposal. MATC has policies including standards, guidelines governing electronic resource use, and firewall and wireless policies. MATC will take reasonable and appropriate steps consistent with current technological developments to make sure that all Protected Information is secure and to safeguard the integrity of records in storage and transmission. MATC will follow current policies, including 9.1.1 Computer Usage Policy, 9.1.4 Clean Desk Policy, and 9.1.5 Telecommuting Policy for all electronic Protected Information by encrypting it for transit.

Management of System Failures

MATC will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of security threats; imaging documents and shredding paper copies; backing up data regularly and storing back-up Information off-site, as well as other reasonable measures to protect the integrity and safety of information systems.

Oversight of Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that MATC determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access Protected Information, the evaluation process shall include the ability of the service provider to safeguard Protected Information. Contracts with service providers may include the following provisions:

- A requirement that the Protected Information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- A requirement that the service provider have documented appropriate safeguards and controls (e.g., SOC2) to protect the Protected Information it receives and that it must promptly report any security incidents that may affect MATC protected information;
- Where appropriate, a requirement that the service provider maintain certain types of insurance to cover potential liability in the event of a security incident;
- Where appropriate, a requirement that the service provider submit to audits of its information security and privacy policies, procedures and controls.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment, especially due to the constantly changing technology and evolving risks. The Coordinators, in consultation with the administration, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, student/customer data sensitivity and internal or external threats to information security.