Monroe Community College

Gramm-Leach-Bliley Act
Information Security Program

Background

The Gramm-Leach-Bliley Act (GLBA) of 1999 mandates that financial institutions must take steps to safeguard the security and confidentiality of customer information. The Federal Trade Commission (FTC) ruled that GLBA applies to institutions of higher education. Compliance with GLBA involves compliance with the privacy provisions of the Act and provisions regarding safeguarding of consumer information. The FTC has said that colleges meet compliance with the privacy provisions of GLBA if they comply with the Family Educational Rights and Privacy Act (FERPA). GLBA specifies requirements for colleges to safeguard non-public customer information with an institutional security program and security plans in specific offices of the college that handle such information. Additionally, Title IV regulations per the Federal Student Aid Program Participation Agreement and the Student Aid Internet Gateway Agreement require colleges to have GLBA safeguards in place.

Designated Security Program Officers

The designated GLBA Information Security Officers for Monroe Community College are the GLBA Compliance Team, including the Chief Information Security Officer, Institutional Compliance Officer, Financial Aid Compliance Director, and FERPA Compliance Officer. The GLBA Compliance Team consists of representation from Technology Services, Institutional Compliance & Internal Audit, Controller's Operations, Student Financial Aid and Registration & Records.

Customer Information

For GLBA and FERPA, the College considers students, employees, and alumni or any other third party engaged in a financial transaction with Monroe Community College as a "customer". GLBA requires safeguarding of customer information for any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form. For these purposes, the term nonpublic financial information shall mean any information:

- A student or other third party provides in order to obtain a financial service from the College,
- About a student or other third party resulting from any transaction with the College involving a financial service, or
- Otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Examples of customer information include addresses, phone numbers, bank and credit card account numbers, date of birth, income and credit histories, details of any financial transactions and social security numbers, in both paper and electronic format.

Elements of the Program

a.) **FERPA** – With respect to the privacy provisions of GLBA, Monroe Community College complies with FERPA as follows:

- MCC publishes a list of directory information annually in the Student Handbook.
- All non-directory information is restricted and only released outside the college with the student's written consent unless there is a legitimate educational interest.

Related college procedures are SUNY Family Educational Rights and Privacy Act (FERPA) Procedures and MCC Student Handbook – Family Educational Rights and Privacy Act (FERPA). There are several links to MCC's FERPA procedures including Student Services homepage, Registration & Records homepage and the A-Z index.

b.) **Risk Identification and Assessment** – Monroe Community College, as part of the GLBA Information Security Program, completed a risk assessment using the NIST 800-171 risk framework. The assessment identified external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The GLBA Compliance Team will rank risks and if appropriate provide a recommendation to minimize key risks to strengthen GLBA compliance. The GLBA Compliance Team will update the Information Security Program annually and when needed due to changes in information security policy and procedures. Results contained MCC's 2018 Risk Assessment Report.

c.) **Employee training and management** – All potential new employees are subject to reference and background checks. New Employees receive training that includes MCC's mission & strategic plan, Title IX, lockdown procedures & emergency communication, and divisional specific training. All College employees, including part-time and temporary employees get specific training by their supervisors about issues of security and sensitive and confidential material used in their respective offices. Annual Cyber Security Awareness Training is mandatory for all employees. The Chief Information Security Officer and staff regularly publish security information in the employee electronic newsletter, the Tribune. Employees who work with customer accounts receive training in the requirements for identity theft prevention. Related college policies and procedures are Password Policy, MCC Acceptable Use of College Technology Policy and Identity Theft Prevention Program Policy and related procedures.

d.) **Physical Safeguards** - Whether the information is stored in paper form or any electronically accessible format, authorized employees use direct control to maintain, store, transmit and other wise handle nonpublic information during business hours. The College distributes papers with nonpublic information via official campus mail, US mail, private mail carrier or department fax machines. Locked file cabinets are used to store documents containing confidential information and confidential information is securely disposed of when no longer needed. A certified recycling vendor is used to securely wipe all data from decommissioned technology equipment, devices and electronic media. Conversations concerning nonpublic information are held in private. Activated screensavers with passwords are used. Key access is limited to authorized College employees only, in the context of College key control governing the distribution of keys. Offices and/or computers are locked when the office will be vacant for an extended length of time. Camera coverage is monitored in areas that are determined to be high risk. Certain offices require key card access. Public Safety further ensures the security of offices after hours by checking that administrative offices are secure. Related College policies and procedures are MCC Employee and Visitor Conduct Policy, MCC Information Technology Security Policy and related procedures and MCC Key Control Policy.

e.) **Records Retention** – MCC departments are responsible for retaining records in accordance with the Records Retention and Disposition Schedule CO-2 and any other legal requirements. Additionally, Archives & Record Management works one-on-one with departments that encounter situations where records retention requirements are not clear. The Archives & Record Management department is responsible for ensuring retention with records they maintain in long-term storage. The facility has a single entrance accessible only by the Archives and Records Management Department. Only the originating department, or owner, of a specific record may access their records. Once a record has reached its minimum legal retention length, Archives & Records Management notifies the originating department and upon approval destroys the records in a secure manner. Destruction of records is done via an industrial shredder. For large scale shredding the College uses Classified Scanning and Shredding recommended by the New York State Archives.

f.) **PCI DSS** -The Payment Card Industry Data Security Standard is a set of security standards MCC accepts and follows when transmitting credit card information across a secure environment.

- On an annual basis, MCC Controller's and CNS Computing complete the self-assessment Questionnaire sent by Security Matrix.
- Security Matrix conducts the PCI scan quarterly and notifies MCC Controller's Office if problems exist.
- All documents related to the PCI scan are stored at Security Matrix.
- Related document is the MCC PCI-DSS Best Practices.

g.) **HIPAA** – MCC Health Services has a Confidentiality and Privacy Statement and Privacy of Medical Records Policy/Procedure that is compliant with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. All staff are oriented to the Policy/Procedure and sign a statement of understanding and agreement upon hire. Annually each member of the Health Services team, including student employees, must read and sign a confidentiality statement and review the HIPAA Statewide Agency Training. New patients receive a Privacy of Medical Records Policy/Procedure and sign the form, confirming receipt of the information. The signed document is stored in the patient medical file. The Privacy Policy notice is also hung prominently in the waiting area and noted on the web page and in office brochures and programs. Health care records are kept separately from academic records and require written permission (Authorization for Release of Medical Information form) for release outside of the College. Medical records are stored via a secure Electronic Medical Record System in the Health Services office. Each member of the Health Services team has their own sign in, if someone leaves the department their sign in is disabled. As required medical records are kept for seven years and then destroyed by deleting them from the system.

h.) **Web Privacy** – MCC does not collect any personal information from individuals visiting monroecc.edu unless provided voluntarily by sending email, completing an online information request form, completing the online application, or completing online registration. MCC limits employee access to personal information collected through monroecc.edu to only those employees who need access to the information in the performance of their official duties. Security procedures including authentication, authorization, monitoring, auditing and encryption are integrated into the design, implementation and day-to-day operations of monroecc.edu. Related college policy is Monroe Community College's Web Privacy Statement.

i.) **Technical Safeguards** –

- **Anti-virus Software**: All MCC PCs run System Center End-Point protection software that protects against malicious software.
- **System Patch Management:** MCC uses a patch management system to apply patches, fixes and hotfixes to Microsoft products. These updates are applied monthly to all MCC PCs and servers.
- **Classroom Imaging Rebuilds:** Rebuilding a classroom images every time a classroom computer is rebooted, which allows a refreshed clean image. This is another way to stop the spread of malware on campus.
- **Laptop Data Encrypt:** MCC owned laptops use an encryption program to encrypt all data stored on the hard drive. This is a precaution in the event the laptop is lost or stolen the data will be unreadable.
- **Nightly Backups:** MCC's performs nightly backups of our network storage. In the event of a loss in data, MCC can retrieve and restore back to a previous night's backup.
- **Virtual Private Network (VPN)**: A VPN allows employees to securely access MCC's systems and data while outside the office.
- **Wi-Fi:** MCC's wireless access uses encryption to securely data access the network.
- **Cloud Vendor Assessment:** Cloud service has many benefits. At the same time, Cloud Service Providers (CSPs) are not bullet proof from hackers/attackers. Therefore, it is crucial that MCC takes proactive steps in protecting MCC data when partnering with CSPs.
    - All CSPs are required to fill out the *Monroe Community College Vendor Assessment Questionnaire*.
    - Check regularly with CSPs regarding their infrastructure or policy changes

- Revise list of cloud services and their providers on an annual basis.
- When it comes to sensitive or classified data, decision needs to be made whether cloud service or in-house systems has appropriate controls.

j.) **Detecting, Preventing and Responding to Attacks** –

- **Firewall and Intrusion Prevention System (IPS):** This appliance protects and secures our network perimeter. It inspects and filters network traffic coming into the college's network and discards any unauthorized network traffic. It provides a virtual wall that protects and hides our internal network from the outside Internet.
- **Email Spam Filter:** This appliance can detect unsolicited and unwanted emails from getting into an MCC Outlook inbox. This serves as another layer of protection against emails that may contain malware.
- **Email Content Filtering**: MCC's email system is configured to prevent SSNs, and credit card numbers from being emailed. It also removes specific file extensions from being delivered or opened. This is another precaution in the spread of malware.
- **Quarterly Vulnerability Scanning**: The College uses several software programs designed to scan our systems and applications and assess them for weaknesses. These vulnerabilities are then addressed in a timely manner.
- **Member of SUNY Security Operations Center (SOC):** SOC provides a Security-as-a-Service 24X7 threat monitoring solution.
- **Information Security Incident Response Plan (ISIRP):** Draft.

<u>**Technology Policies, Procedures and Best Practices**</u>

- **Password Policy:** MCC enforces a strong password policy for all employees who access MCC's systems.
- **Acceptable Use of College Technologies Policy:** MCC computer facilities and systems are intended for appropriate college-related work.
- **Information Technology Security Policy:** Establishes the overall intent of Monroe Community College to support and promote information security in all its practices.
- **Mobile Device Acceptable Use Policy:** Establish the criteria governing the authorized use of personally owned or Monroe Community College (MCC) owned mobile devices (smartphone, laptop, notebook, iPad tablet, USB storage, etc.). (Draft)
- **Cyber Security Awareness and Education Policy:** All employee users required to complete regular training.
- **Confidentiality Agreement:** Every employee is responsible for maintaining the confidentiality of data to which they have access. (Draft)
- **Privileged Account agreement:** Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. (Draft)
- **Wireless Policy:** Specifies the conditions that wireless infrastructure and devices must satisfy to connect to MCC wireless networks. (Draft)

- **Data Risk Classification Policy:** MCC has classified its data into three risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it. (Draft)
- **Cloud Vendor Assessment Questionnaire:** A questionnaire to send to potential or current vendor for Monroe Community College in order to evaluate the organization's information security program.
- **PCI-DSS Best Practices:** Responsibilities of department personnel who process payment Card Transaction. (Draft)

Violations

Employee violations of MCC Acceptable Use of College Technology Policy will be investigated and appropriate disciplinary action will be taken as determined by college and legal authorities per section 7.1 of MCC Acceptable Use of College Technology Policy.

Overseeing Service Providers

At the onset of all new contracts, MCC requires vendors to complete a questionnaire that includes Company Information, Project Information, and Security Questionnaire. MCC uses this information to evaluate whether the vendor has access to non-public information. Contracts with service providers, who have access to Monroe Community College non-public customer information, include specific provisions regarding maintaining appropriate safeguards. The College does not approve vendors that cannot maintain appropriate safeguards. Related College policies are the MCC College Contracts Policy and Cloud Vendor Questionnaire.

Program Adjustments

The GLBA Information Security Program will be subject to periodic review and adjustment, at least annually. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the GLBA Compliance Team. The Team will review the standards set forth in this program and recommend updates and revisions as necessary to reflect changes in law, technology, the sensitivity of student/customer information, and/or internal or external threats to information security.

Communication

The GLBA Information Security Program shall be published in *Online Forms and Documents* within the *Employee Essentials* tab of myMCC web portal and communication to the college community will occur via the Tribune electronic newsletter. Additionally, the Program will be sent directly to the President and Vice President of each division. Questions regarding MCC's GLBA Information Security Program should be directed to the Chief Information Security Officer or Compliance Officer at InfoSecurity@monroecc.edu.

Related Policies & Other Documents

SUNY:

Family Educational Rights and Privacy Act (FERPA) Procedures

MCC:

Acceptable Use of College Technology Policy

Authorization for Release of Medical Information form

College Contracts Policy

Confidentiality and Privacy at MCC Health Services Statement

Cyber Security Awareness and Education Policy

Data Risk Classification Policy

Employee and Visitor Conduct Policy

FERPA Procedures

Identity Theft Prevention Program Policy and Procedure

Information Technology Security Policy and Procedures

Key Control Policy

Mobile Devise Acceptable Use Policy

Password Policy

Payment Card Industry Data Security Standards (PCI-DSS) Best Practices

Privacy of Medical Records Policy/Procedure

Vendor Questionnaire

Web Privacy Statement

Wireless Policy

2018 Risk Assessment Report