Information Security Program

…….

ESTABLISH AND MAINTAIN AN INFORMATION SECURITY PROGRAM

According to The Gramm-Leach-Bliley Act (Public Law 106-102), consumers are provided the right to know the information-sharing practices of PII at a financial institution. This policy is published on the Messenger College website and a notice of the location is provided annually to students.

Personally Identifiable Information (PII) is defined as a person's first and last name OR first initial and last name, and at least ONE of the following:

1. Social Security Number
2. Date and place of birth
3. Driver's license or identification card number
4. Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account

The purpose of MC's Information Security Program is to:

1. Establish safeguards regarding the use of MC's information resources.
2. Protect the privacy of individuals by preserving the confidentiality of personally identifiable information.
3. Ensure compliance with applicable state and federal regulations regarding management of risks to and the security of information resources.
4. Appropriately reduce the collection, use, and disclosure of SSN and paper records.
5. Establish accountability.
6. Educate individuals regarding their responsibilities associated with use and management of MC's information resources.

Information resources residing in MC's systems are appropriately managed and protected against accidental or unauthorized access, disclosure, modification, or destruction. MC assures the availability, confidentiality, and integrity of these resources. Information is protected in the following ways:

1. Accountability

- The Chief Information Security Officer has oversight of information resources and ensures the institution's compliance with this policy and associated standards.
- Duties of the Chief Information Security Officer include:
  - provide leadership, strategic direction, and coordination for MC security protection.
  - chair and hold meetings of the Information Security Program committee.
  - conduct at least one committee meeting per year.
  - develop and oversee MC's information security compliance.
  - ensure performance of risk assessments for MC's process and storage of confidential data.

- recommend the acquisition of cyber security tools and resources as necessary.
- report the effectiveness of security strategies to the Board of Governors.

2. Acceptable use of information resources

- MC's information resources are provided for conducting the business of the College. Users are permitted to access the information resources for official duties related to their position.
- Users have no expectation of privacy regarding the data they create, send, receive, or store on MC-owned computers, servers, or other information resources owned by MC. MC may access and monitor its information resources for any purpose consistent with MC's duties or mission without notice.
- When transmitting information containing PII, employees must use a high degree of confidentiality and care. Information containing PII may not be transmitted by an MC employee via fax (unless immediate receipt can be assured) or email (unless encrypted).

3. Information Security Programs

The Chief Information Security Officer shall maintain and implement the following program objectives:

- Annual risk /vulnerability assessment with strategies for improvement.
- Current inventory of institution-owned computing devices.
- Annual action plan, training plan and monitoring plan; and,
- An annual report to the Board of Governors.

4. Access management

The information resources at Messenger College are managed by the following safeguards:

- Access to information resources is restricted to authorized users.
- A uniquely identifiable password-protected user account is created for all system users.
- Inactive accounts are disabled.
- The use of secure and/or encrypted connections is required when downloading protected information across the internet.
- Employees may not disclose confidential data to unauthorized persons or institutions except as required or prevented by law, by the consent of the data owner, or where the third party is the contractor or agent for the institution.

5. Backup and Disaster Recovery

- Hard copy files are secured in locked onsite storage under supervised access and disposed of according to the Record Retention Destruction Policy BA-37.
- In order to prevent loss of information resources in the event of a disaster, employees are required to routinely backup information on a secured storage device, to be stored offsite.

6. Safeguarding Data

- Password protection is provided for desktop computers and laptop computers.
- College data may not be stored on personally owned storage servers/services or devices.
- Electronic data downloaded to portable college-owned devices must be properly and timely deleted.

7. Security incident management

- Any security incidents must be reported to and documented by the Chief Information Security Officer and reported to the IT Committee.
- All employees must promptly report any unauthorized or inappropriate disclosure of data to their supervisor, or the Chief Information Security Officer.

8. Use and protection of Social Security Numbers

- The use of all or part of the social security number is never used as the individual's primary ID number.
- Social security numbers are stored as confidential data and are only used for verification of identity.
- Confidential information is never permitted to be publicly displayed or posted.
- Social security numbers are not displayed on documents that are accessible to individuals who do not have a business reason to access the document.
- If documents with social security numbers are distributed via mail, the social security number is placed in an envelope in a way to ensure that no part is visible from the outside.
- MC prohibits employees from sending or requesting others to send PII (i.e., social security numbers) by email (unless encrypted) or fax (unless immediate receipt can be assured.

9. Passwords

- Passwords are used to control access to information resources. Issuing or resetting passwords requires ensuring the user's identity.
- Users may not share passwords or similar information, or devices used for institutional business.

10. Physical security

- Facilities containing information resources have controlled visitor access (i.e., advanced scheduling, login of visits, escorts when necessary, etc.).
- Employees are required to lock all MC devices when not in use.
- When employees have a change in employment status, the institution will restrict access (i.e., collect keys, equipment, etc.).
- Hard copies of records containing PII are kept in locked offices or in locked cabinets with restricted access.

11. Security training

- MC provides initial and recurring training on user responsibilities, common threats, risk behaviors, regulatory and institutional requirements regarding acceptable use and proper handling of information resources and confidential data. Training will also include how to report an incident.
- Recurring training shall take place at least every two years. New employees must complete the initial training within 30 days of hire.

12. Third Party Services

- The protection of information resources is included in the procurement decision-making process of third-party servicers.
- Records of the protection provided by third party servicers is maintained by the Chief Information Security Officer.
- Third party contractors or agents of the college shall provide additional information security policies and procedures to protect information resources.

13. Disciplinary actions

- Violations of this policy by faculty, staff, and/or students are subject to disciplinary action. Certain violations may also result in civil action or referral for criminal prosecution.