

---

# Maine Maritime Academy

## Information Technology Department

### Internet Information Security Policy

#### 1. Purpose

This policy outlines the guidelines for protecting the privacy and security of sensitive financial information in accordance with the **Gramm-Leach-Bliley Act (GLBA)**. The purpose of this policy is to ensure that all electronic systems, networks, and activities involving personal and financial information are secure, preventing unauthorized access, misuse, and breaches.

#### 2. Scope

This policy applies to all faculty, staff, contractors, and students who access or handle sensitive information, including financial records, credit reports, personal data, and other types of non-public information (NPI), in accordance with the GLBA. It covers all devices, systems, and networks used to store, transmit, or process such information.

#### 3. Definition of Terms

- **Non-Public Personal Information (NPI):** Any personal information that is not publicly available and that identifies an individual, such as financial information, Social Security numbers, or account details.
- **GLBA:** The Gramm-Leach-Bliley Act, a U.S. federal law that mandates financial institutions to safeguard the privacy and security of consumers' personal financial information.

#### 4. Data Classification and Protection

- All non-public personal information (NPI) must be classified and labeled to ensure proper handling and security.
- NPI may include, but is not limited to:
  - Student financial aid information
  - Billing and payment details
  - Bank account or credit card information
  - Tax and income records
  - Social Security numbers

##### 4.1 Data Encryption

- All NPI stored on college systems or transmitted over networks must be encrypted using industry-standard encryption protocols (e.g., AES-256, TLS).
- Any data transmitted outside the college network, including email, must be encrypted to ensure confidentiality.

## **4.2 Data Access Control**

- Access to NPI shall be granted on a need-to-know basis. Only authorized individuals (e.g., staff members with financial, administrative, or legal responsibilities) should have access to such data.
- Role-based access control (RBAC) must be implemented to limit the scope of access based on job functions.
- Employees and contractors must use strong, unique passwords and multi-factor authentication (MFA) when accessing systems containing NPI.

## **4.3 Data Retention and Disposal**

- NPI shall be retained only for as long as necessary for business or legal purposes, in accordance with retention schedules.
- Upon disposal, all physical and electronic records containing NPI must be securely destroyed, using methods such as shredding paper records or securely wiping electronic devices.

## **5. Risk Assessment and Monitoring**

- A periodic risk assessment will be conducted to identify vulnerabilities that could potentially compromise the security of NPI.
- Vulnerabilities identified in systems, networks, or processes must be addressed through appropriate security measures, such as patching software, upgrading security hardware, or changing protocols.
- Continuous monitoring tools shall be employed to detect unauthorized access or anomalous activities on systems that handle NPI. Any suspicious activity will be investigated and acted upon promptly.

## **6. Employee Training and Awareness**

- All employees with access to NPI must undergo mandatory security training at the time of hire and annually thereafter. Training will cover the following:
  - Recognizing and reporting security threats (phishing, malware, social engineering, etc.)
  - Safe handling and storage of NPI
  - College policies regarding information security and privacy
- Employees will be made aware of their responsibilities under the GLBA and the potential consequences of non-compliance.

## 7. Incident Response and Reporting

- A formal incident response plan shall be established to address any breaches of NPI or violations of security protocols.
- Employees must immediately report any suspected or actual security incidents, including data breaches, to the IT security team and the designated privacy officer.
- In the event of a breach of NPI, the college will notify affected individuals in accordance with the notification requirements of the GLBA and any applicable state laws.

## 8. Third-Party Service Providers

- Any third-party vendors or contractors who have access to NPI must be thoroughly vetted for their ability to maintain appropriate security controls in compliance with GLBA.
- Contracts with third-party service providers must include clauses outlining the provider's obligations regarding the protection of NPI, including data security and breach notification.

## 9. Compliance with GLBA

The college is committed to adhering to the requirements set forth by the Gramm-Leach-Bliley Act:

- **Privacy Rule:** Protect the confidentiality of NPI by ensuring it is not disclosed to unauthorized parties without consent, except as allowed by law.
- **Safeguards Rule:** Establish and maintain physical, technical, and administrative safeguards to protect the security and confidentiality of NPI.
- **Pretexting Protection:** The college will implement policies to protect against pretexting (the practice of obtaining personal information under false pretenses).

## 10. Enforcement and Consequences

- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.
- In addition to internal consequences, individuals or entities that violate this policy may be subject to legal penalties under applicable federal or state laws.

## 11. Policy Review and Updates

- This policy will be reviewed annually, or sooner if necessary, to ensure it remains up-to-date with applicable laws, regulations, and security practices.
- Updates to this policy will be communicated to all employees and relevant stakeholders.

## Appendix A: Relevant GLBA Sections

- **Section 501(b) (Safeguard Rule):** Requires financial institutions to develop and implement written information security programs to safeguard customer information.
  - **Section 502 (Privacy Rule):** Limits the disclosure of non-public personal information and requires financial institutions to establish privacy policies.
-