Data Governance Policy

1: Purpose

This document outlines Maine Maritime Academy's (MMA) requirements for the use of institutional data and systems. The purpose of this document is to provide a framework for ensuring that institutional data are protected from unauthorized disclosure while ensuring the institution remains in compliance with Federal and State laws, rules, and regulations.

2: Scope

This document applies to the following:

- Employees of Maine Maritime Academy
- Students attending Maine Maritime Academy
- All data created, stored, processed, or transmitted by the Academy
- All data provided to 3rd party and affiliated organizations of the Academy

3: Definitions

Protected Information: This includes proprietary, personal, and FERPA data. It includes all data covered by relevant and applicable data protection statutes, laws, rules, and regulations.

Proprietary Data: Data created by the institution that, if subject to unauthorized release, would harm the institution's reputation, interfere with the normal operations of the institution, or would otherwise negatively affect the operations and/or standing of the institution.

Personal Data: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

FERPA Data: Information subject to the Family Educational Rights and Privacy Act of 1974. This includes, but is not limited to grades, evaluation data, or academic transcripts.

Data Owner: Individual responsible for ensuring the protection, classification, quality, and security of data.

Data Custodian: Individual or team responsible for maintaining and securing the institution's data systems.

Principle of Least Privilege: Systems, users, or processes acting on behalf of users are granted only the specific permissions needed to complete their tasks.

4: Data Classification

All protected information shall be classified into one of the following categories:

- Restricted: Highly sensitive data requiring the strictest controls. This includes, but is not limited to financial data, government identification numbers, and FERPA data.
- Confidential: Sensitive information not intended for public release. This includes but is not limited to employee records and internal reports.
- Internal Use: Information intended for operational use.
- Public: Data or information approved for public release.

5: Data Handling and Processing Requirements

5.1: Collection

The collection of data shall be restricted to only data necessary for legitimate institutional purposes. When collecting these data, the institution must inform individuals of the purpose of the data collection, if possible.

5.2: Storage

Protected information shall only be stored on approved Academy applications, devices, or systems. Data must be encrypted, both at rest and in motion, whenever possible using industry standard practices.

5.3: Transmission

When protected data being sent from one system or individual to another, either internally or externally, the following shall apply:

- Data transmission shall be done using a secure protocol. This includes, but is not limited to:
    - HTTPS, SFTP, MMA VPN
    - Secure Mail
    - Transfer via shared drive or through contracted cloud file storage provider

5.4: Access Control

All access to systems holding protected information shall adhere to the following guidelines:

- The principle of least privilege shall be enforced.

- Multi-factor authentication shall be enforced when possible.
- Permissions for access to protected information shall be reviewed annually.

5.5 Retention and Destruction

Protected data shall be retained by the institution for at least a length of time required by any federal or state laws, rules, regulations.

When data are required to be destroyed, it must be destroyed using a method in which it's recovery is made impossible. This includes the shredding of physical documents, securely wiping physical storage devices, or by any other approved means of data destruction.

6: Security Controls

The following safeguards, at minimum, shall be employed by the Academy:

- Firewalls
    - These firewalls shall be kept up to date and include any critical and important patches.
    - Firewall policies shall be reviewed annually.
- Intrusion Detection Systems
- Patch management
    - Patches for servers and endpoints shall be applied on a regular basis.
    - Critical patches shall be applied upon their release.
- Vulnerability assessments and penetration testing
    - Regular assessments of MMA's information security shall be conducted on a regular basis.
    - Internal or 3rd party penetration testing shall be conducted on a regular basis.
- Network segmentation
    - Critical systems must be segmented from any public or unauthenticated networks.
- Backup and disaster recovery
    - MMA shall maintain backups for critical systems.
    - MMA shall maintain a disaster recovery plan and review said plan annually.

7: Incident Response

7.1: Reporting

Any suspected or confirmed breaches of the Data Governance Policy must be reported immediately to the Information Systems Security Officer, Chief Technology Officer, or their representative.

7.2: Response

Once a breach has been reported, the institution shall:

- Contain and/or mitigate the incident in accordance to the Academy's incident response plan.
- Investigate the root cause of the breach.
- Notify affected parties in accordance with any applicable laws, rules, or regulations.
- Report the breach findings to institutional leadership.

7.3: Documentation

Details of the breach, including root cause, response details, and after-action information shall be kept and reviewed for continuous improvement.

8: Compliance and Legal Requirements

MMA shall comply with all applicable laws, rules, and regulations. These include, but are not limited:

- The Family Educational Rights and Privacy Act of 1974.
- Maine regulations and laws pertaining to data breach notifications.

9: Roles and Responsibilities

9.1: Data Owners

Individuals or job descriptions designated as Data Owners shall classify and define data generated by their department.

9.2: IT Department

MMA's IT Department shall implement and maintain the systems by which data is transmitted and disclosed. This includes regular training on data handling best practices.

9.3: Information Security Personnel

These personnel are responsible for the management and maintenance of security controls and systems, including the security controls listed in Section 6 of this policy. Additionally, these personnel are responsible for the regular review of this policy.

10: Training and Awareness

Regular training and awareness programs shall be performed in accordance with the Cybersecurity Awareness Training policy.

11: Third Party Risk Management

Any system or vendors processing protected information must sign data protection agreements. When any new systems or vendors are being evaluated, a risk assessment shall be performed.

The use of any system or vendor not contracted or a signatory to the Academy's data protection requirements shall be considered a breach of this policy. This includes, but is not limited to:

- Protected information uploaded to a 3rd party cloud system not approved by the institution.
- Protected information analyzed or in any way processed by an Artificial Intelligence platform not approved by the institution.

12: Policy Enforcement

The Data Governance Policy follows the progressive discipline standards of the collective bargaining agreements.

The Academy agrees that it will follow the principle of progressive discipline for minor offenses prior to effecting a discharge or suspension without pay of a unit member. Counseling, while encouraged, is not part of the discipline process. For purposes of this Article, progressive discipline shall be defined as:

1. first written warning
2. second written warning
3. suspension without pay
4. discharge

Notice of minor discipline (Written Warnings) shall remain in effect for a period of not more than one (1) year from the date of the occurrence upon which a complaint and warning is based, provided that the unit member has received no other related disciplines during

such period. Records of suspensions shall remain in effect for a period of not more than two (2) years from the date of the occurrence. Supervisory commendations and employee rebuttals may be placed in a Unit member's personnel file.

13: Policy Review

The Data Governance Policy shall be reviewed regularly. This policy shall be updated to reflect any changes in industry best practice, technology, or Institutional need.