Monroe Community College
STATE UNIVERSITY OF NEW YORK

7.4 Data Classification Policy

Category: Technology
Name of Responsible Office: Technology Services
Title of Responsible Executive: CFO and Vice President, Administrative Services
Date Established: March 7, 2022
Date Last Approved:

Summary

Monroe Community College is committed to the confidentiality, integrity and availability of information important to the college's mission. The purpose of this policy is to define a framework for identifying, classifying and handling institutional data based on its level of sensitivity, value and criticality to Monroe Community College (MCC).

Data classification, in the context of information security, is the classification of data based on its impact on the college should that data be disclosed, altered, or destroyed without authorization. Classification of data helps determine what security controls are appropriate for safeguarding that data, and also positions the college to remain in compliance with current and emerging privacy laws and regulations.

MCC has established the requirements enumerated below regarding the classification of data to protect the institution's information.

Policy

Scope

The scope of this policy includes all information assets governed by MCC.

Institutional data are any data related to the business of the college, including but not limited to: financial, employee, student, and alumni information. It includes data maintained at the department level as well as centrally, regardless of the media or system on which they reside. Institutional data include records that are stored in on-premise college data systems, as well as systems and/or applications hosted by other providers via public internet service providers or private cloud.

Data Ownership and Accountability

Data owners are identified as the individuals, roles or committees primarily responsible for information assets. These individuals are responsible for:

- Identifying the college's information assets under their areas of supervision; and
- Maintaining an accurate and complete inventory for data classification and handling purposes; and
- Controlling access to the data under their areas of supervision

Data Owners are accountable for ensuring that their information assets receive an initial classification upon creation and a re-classification whenever reasonable. Additionally, data owners are responsible for reporting deficiencies in security controls to Risk Management.

Data Custodians manage the actual data in terms of where it is stored and how it is transmitted and to where, through the management of systems, servers, networks and types of storage. Although this role provisions data access, it is done per the direction and approval of the data owner.

Data Users are those who have been given authorization to access specific data. Data users are required to comply with all policies and guidelines established by the data owners when handling college data, as well as with all applicable laws. These include but are not limited to the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA).

Data Classification

Classification of data is performed by the data asset owner based on specific, finite criteria. Refer to the Data Classification and Handling Procedure to determine how data should be classified. Data classifications are defined as follows:

- Restricted – Information whose loss, corruption, or unauthorized disclosure would cause severe financial, legal or reputational harm to the college and/or to its constituents, such as identity or financial fraud, significant revenue loss, or the unavailability of critical systems or services. Restricted data include data protected by state, federal, and/or international privacy regulations and confidentiality agreements. In the event of a restricted data breach, federal and/or state breach notification would be required. The 2005 New York State *Security Breach and Notification Act* and the 2019 New York State SHIELD (*Stop Hacks and Improve Electronic Data Security*) Act require the college to disclose any breach of data to the affected individuals.

  Common examples of Restricted data include, but are not limited to: social security number, bank account/credit card/debit card numbers, HIPAA protected health information (PHI), and information systems authentication data.

  The highest level of security controls should be applied to Restricted data.

- Private – Information whose loss, corruption, or unauthorized disclosure would likely cause moderate personal, financial, operational or reputational harm to the college and/or to its constituents, but would not require federal or state breach notification.

  Common examples include, but are not limited to: HR employment records, unpublished research data, Family Educational Rights and Privacy Act (FERPA)-protected student records, electronic records that are specifically exempted from disclosure law, IT infrastructure information, data protected by nondisclosure agreements, law enforcement investigation data, and student disciplinary information.

  Private data are relevant to internal operations and are not readily available to the public.

  By default, all college data that are not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data, as described in the Data Classification and Handling Procedure.

- Public – Information whose loss, corruption, or unauthorized disclosure would not cause personal, financial or reputational harm to the college and/or to its constituents. This category also includes general access data, such as that available on unauthenticated portions of the college's website.

  Public data have no requirements for confidentiality; however, reasonable measures should be taken to ensure their accuracy.

  Directory Information is classified as Public data (unless a student restricts its release under FERPA).

  Faculty and Staff Directory Information

  Faculty and Staff Directory Information is defined as the following:

  - Name
  - Email address
  - Current position title

- Date of hire
- Date of separation
- Department of assignment
- Office telephone number
- Office address (campus, building, room)

Student Directory Information

Student Directory Information is defined as the following:

- Name of student
- Email address
- Picture
- Major fields of study
- Dates of attendance
- Full- or Part-Time status
- Awards and degrees received
- Most recent previous educational agency attended
- Participation in recognized activities and sports
- Weight and height of members of athletic teams

Data Handling

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention schedules and destruction procedures. The specific methods are documented in the Data Classification and Handling Procedure.

Re-Classification

A re-evaluation of classified data assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired or destroyed.

Classification Inheritance

Logical or physical assets that "contain" a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

Enforcement

Violations of this policy may result in the immediate suspension and/or revocation of information technology resource privileges in order to protect the integrity, security or functionality of computing resources and/or to protect the college from liability. Students may also be subject to disciplinary action in accordance with the Student Code of Conduct. Employees may be subject to college disciplinary action in accordance with all applicable collective bargaining agreements. Violations of state and/or federal laws in the use of the college's data may also result in criminal prosecution of the individual(s) liable as well as civil penalties.

Applicability

All faculty, staff, students, college affiliates and third parties who have authorization to access or utilize institutional data to process, store and/or transmit information for or on behalf of MCC shall be subject to these requirements.

Exceptions

Exceptions to this policy must be approved in advance by the CFO/Vice President, Administrative Services, at the request of the data asset owner. Approved exceptions must be reviewed and re-approved by the asset owner annually.

Responsibility

CFO/Vice President, Administrative Services