**University of Massachusetts Lowell**

| | |
|---|---|
| **Policy Title:** | Data Classification Policy |
| **Policy Number:** | IT-5-106 |
| **Effective As Of:** | February 1, 2017 |
| **Next Review Date:** | February 1, 2018 |
| **Responsible Office:** | Information Technology |
| **Responsible Position:** | Information Security Officer |

## I. POLICY STATEMENT

Any UMass Lowell employee who uses, stores or transmits data has a responsibility to maintain and safeguard such data. For purposes of this policy, data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on UMass Lowell owned or contracted computer resources.

The first step in establishing the safeguards that are required for particular types of data is to determine the level of sensitivity applicable to particular data. Data classification is a method of assigning such levels and thereby determining the extent to which the Data needs to be controlled and secured.

This guideline defines four classifications into which University Data can be divided:

- Restricted
- Confidential
- Operational Use Only
- Unclassified (Public)

University Data that is considered Unclassified may be disclosed to any person regardless of their affiliation with the University. All other University Data is considered Sensitive Information and must be protected appropriately. The Data Protection Requirements specifies the level of security protection that are required for each classification of data. Everyone with access to University Data should exercise good judgement in handling sensitive information and seek guidance from management as needed. Even though employees, faculty, staff may have access to University Data, use for research purposes must be reviewed and approved by the Institutional Review Board.

## II. PURPOSE

The purpose of this policy is to identify the different types of data, to provide guidelines and examples for each type of data, and to establish the default classification for data.

## III. SCOPE

This policy covers all data produced, collected or used by UMass Lowell, its employees, student workers, consultants, or agents during the course of University business. It affects all department heads, chairs, faculty, and staff responsible for ownership or oversight of UMass Lowell data.

The University must adhere to the standards detailed in this document, except where such adherence would conflict with the Public Records Law or other laws, regulations, or policies. Additional references that colleges may find useful as they classify data are listed at the end of this document.

## IV. DEFINITIONS

**Controlled Unclassified Information (CUI)** is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. Examples likely to be found at UML include export controlled information, health information, and student records.

**HIPAA**- The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

**FERPA**- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

**Export Controlled Technology/Data –** U.S. export controls restrict the dissemination of covered technology and data outside of the U.S., as well as to certain foreign nationals even within the U.S. Export controls commonly encountered at UML include those under the U.S. Department of Commerce's Export Administration Regulations (EAR), the U.S. Department of State's International Traffic in Arms Regulations (ITAR), and the U.S. Department of Energy.

**Gramm-Leach-Bliley Act (GLB)** - also known as the Financial Services Modernization Act of 1999, GLB compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

**Data Owner:** The Data Owner has policy-level responsibility for establishing rules and use of data based on applied classification. UMass Lowell Senior Level Management is ultimately the Data Owner and is responsible for assigning the classification, ensuring the protection and establishing appropriate use of the school's data. Individuals within UMass Lowell may be delegated some portion of this responsibility on behalf of the Senior Leadership. The Data Owner is also responsible for assigning individuals to the following roles.

**Data Manager**: The Data Manager develops general procedures and guidelines for the management, security and access to data, as appropriate.

**Data Steward:** The Data Steward has custodial responsibilities for managing the data for the day-to-day, operational-level functions on behalf of the Data Owner as established by the Data Manager.

**Data User:** A Data User is any individual who is eligible and authorized to access and use the data.

## V. PROCEDURES

A. Data Classification Scheme

UMass Lowell Departments must classify their data into at least one of the four levels of classifications. Each category denotes a unique level of sensitivity and has specific access and handling requirements.

1. ***Restricted Data – Very High Sensitivity****:* any information protected by federal, state or local laws and regulations or industry standards, such as HIPAA, HITECH, FERPA, ITAR, Export Admissions Regulations, similar state laws and PCI-DSS. This category is subject to the most restricted distribution and must be protected at all times based upon regulatory compliance. Compromise of Restricted Data could result in legal actions or fines and may require reporting to vendors, federal and state agencies.

   For purposes of this Policy and the other Information Security Policies, Restricted Data include, but are not limited to:

   ***Personally Identifiable Information (PII)****:* any information about an individual that (a) can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name or biometric records, (b) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual and (c) is protected by federal, state or local laws and regulation or industry standards.

   ***Protected Health Information (PHI)****:* any information processed, transmitted or stored by a Covered Entity that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. The University's Office of the General Counsel is responsible for determining whether particular information maintained or disclosed by UMass Lowell constitutes PHI.

2. ***Confidential Data – High Sensitivity****:* any information that is contractually protected as confidential by law or by contract and any other information that is considered by the University appropriate for confidential treatment. Such data should not be copied or removed from UMass Lowell operational control without authorized permission. High sensitivity data is subject to restricted distribution and must be protected at all times. Compromise of high sensitivity data could damage the mission, safety or integrity of UMass Lowell, its staff or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

   For purposes of this Policy and the other Information Security Policies, Confidential Data include, but are not limited to:

   - Student education records that are directly related to prior, current and prospective University students and maintained by UMass Lowell or an

entity acting on UMass Lowell's behalf, but not including (a) "directory information", such as a student's name, address, degrees and awards, subject to certain requirements as specified in FERPA and the University FERPA policies or (b) such records disclosed to school officials with legitimate educational interests or to organizations conducting certain studies on UMass Lowell's behalf.

- HR Employee files
- Non-public personal and financial data about donors
- Information received under grants and contracts subject to confidentiality requirements
- Law enforcement or court records and confidential investigation records
- Citizen or immigrations status
- Unpublished research data
- Unpublished University financial information, strategic plans and real estate or facility development plans
- Information on facilities security systems
- Nonpublic intellectual property, including invention disclosures and patent applications
- Applicant financial information

3. **Operational Use Only Data – Medium/Moderate Sensitivity**: any information that is proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data. Release of this data must be approved prior to the dissemination out UMass Lowell. Its compromise may inconvenience a department, but it unlikely to result in breach of confidentiality, loss of value, or serious damage to integrity. This information is critical to the University's academic, research, and business operations that require a higher degree of handling than unclassified (public) data.

   For purposes of this Policy and the other Information Security Policies, Operational Use Data include, but are not limited to:

   - Internal operating procedures and operational manuals
   - Internal memoranda, emails, reports and other documents
   - Technical documents such as system configurations and floor plans

4. **Unclassified (Public) Data – Low Sensitivity**: any information that may or must be made available to the general public, with no legal restrictions on its access or use. Security at this level is the minimum required by UMass Lowell to protect the integrity and availability of this data.

   For purposes of this Policy and other Information Security Policies, Public Data include, but are not limited to:

   - General access data on the university's website www.uml.edu
   - University financial statements and other reports filed with federal or state governments and generally available to the public
   - Copyrighted materials that are publicly available

- Directory information under FERPA

B. Required Considerations for Classification

The considerations listed below must be evaluated by UMass Lowell departments when assigning classifications to their data.

1. ***Laws and Regulations***
   UMass Lowell departments are required to ensure that all laws, regulations, policies and standards to which their data is subject are met. Questions regarding laws, regulations, policies and standards that apply to specific agencies and departments should be directed to UMass Lowell or department counsel.

2. ***Potential harm to the individuals to whom the data pertains***
   It is imperative to take into consideration any potential harm or adverse impact that the compromise of data may have on the parties to whom the data pertains. This consideration pertains to, but is not limited to patient data, personally identifiable information and medical information.

3. ***Risk of loss of confidentiality***
   Confidentiality has been defined as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Therefore, in appropriately assigning data with a classification level, departments must evaluate what the risk is for unauthorized access to classified data and what likely impact that loss would have.

4. ***UMass Lowell Mission and Business Objectives***
   UMass Lowell with unique missions and business objectives should take those needs into consideration when evaluating their data classifications. In some cases, the University may be obligated to share as much of their data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the department to ensure that those objectives are met, adequate controls need to be in place and in effect to address data integrity, security and availability.

5. ***Data Sharing Agreements and Contractual Requirements***
   Interagency Service Agreements (ISAs), Memoranda of Understanding (MOU's), grants, contracts and other written agreements between agencies and external entities may include agreements regarding data sharing and the use, disclosure and maintenance of data, as determined by the data classification of the Data Owner. The recipient UMass Lowell or department's data classification must align with any such requirements. Further, if an agreement states that the recipient department may further share the data, the subsequent recipients must adhere to the requirements of the original classification, unless the data has been de-identified or otherwise modified such that a different classification is required.

6. ***Intellectual Property***
   Departments must take into consideration any intellectual property rights owned by an entity other than the department while implementing and evaluating their data classification assignments.

## VI. RESPONSIBILTY

Information Technology is the responsible organization for implementing the provisions of this policy. The University's Chief Information Officer and the Information Security Officer are the designated point of contacts.

## VII. ATTACHMENTS

Appendix A – Examples of Restricted Data
Appendix B – Data Classification Matrix
Appendix C – Data Classification – Storage Options

## VIII. RELATED POLICES, PRODEDURES AND ANNOUNCEMENTS

ISO: International Standards Organization

FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems

FIPS PUB 140-2: Security Requirements for Cryptographic Modules

NIST 800-60: Guide for Mapping Types of Information & Information Systems to Security Categories

NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Fair Information Practices Act: Mass. Gen. L. Ch. 66A

Executive Order 504: Executive Order regarding security and confidentiality of personal information. Public Records Division: Public records resources as provided by the Secretary of the Commonwealth

Massachusetts Identity Theft Law: Law relative to Security Freezes and Notification of Data Breaches

Family Educational Rights and Privacy Act (FERPA): The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Mass. Gen. L. 93H: Commonwealth of Massachusetts Law that protects residents' personal information

201CMR17: Standards for the protection of personal information of residents of the Commonwealth.

HIPAA: Health Insurance Portability and Accountability Act for protection and confidentiality handling of health information

PCI: The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment.

## A P P E N D I X  A

**Examples of Restricted Data**

Examples of PII include, but are not limited to, any information concerning a natural person that can be used to identify such natural person, such as name, number, personal mark or other identifier, in combination with any one or more of the following:

- Social security number
- Driver's license number or non-driver identification card number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Ethnicity

Examples of PHI include, but are not limited to, any health information about an individual, in combination with any one or more of the following:

- Name
- Geographic subdivision smaller than a state
- Any element of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date or date of death
- Telephone number
- Fax number
- Electronic mail address
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Vehicle identifier and serial number, including license plate number
- Device identifier and serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifier, including finger and voice print
- Full face photographic image and any comparable image
- Any other unique identifying number, characteristic, code or combination that allows identification of an individual.