I. POLICY STATEMENT

Colleges, departments, and business functions are required to employ University-approved encryption solutions to preserve the confidentiality, integrity, and accessibility to, University data classified as ‘Restricted and/or Confidential’ where this data is processed, stored or transmitted using University-approved systems.

II. PURPOSE

The purpose of this policy is to establish the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption.

III. SCOPE

This policy applies to all employees, contractors, vendors, and any others (including 3rd parties) entrusted with University Restricted and/or Confidential data.

IV. DEFINITIONS

*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 required 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.

**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.

**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.

**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](http://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

**V. PROCEDURES**

A. Devices and Media Requiring Encryption

Encryption is required for all laptops, workstations, and portable drives that may be used to store or access UMass Lowell Restricted and/or Confidential data. IT will provide, install, configure, and support encryption where it is needed. Departments who have a laptop, workstation, or portable drive that need to be encrypted should contact the IT Information Security team at [infosec@uml.edu](mailto:infosec@uml.edu) or contact the IT Service desk at 978-934-4357 (help@uml.edu).
B. Electronic Data Transfers

Any transfer of unencrypted UML Restricted data or UML Confidential data must take place via an encrypted channel. Encrypted Restricted data or UML Confidential data may be transmitted via encrypted or unencrypted channels. All email communications that involve email addresses outside of UMass Lowell use an unencrypted channel, and therefore require that messages containing UML Restricted and/or Confidential data be encrypted.

Approved methods of encrypting electronic data transfers are as follows:

- Transport Layer Security (TLS1.1 TLS1.2)
- SSH File Transport Protocol (SFTP)
- Connecting via an IT-approved Virtual Private Network (VPN)
- Proofpoint Secure Email Service

If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual. Email messages containing encrypted data may never include the password in the same message as the encrypted data. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact the IT Information Security team at infosec@uml.edu.

C. Physical Transfer of Electronic Data

Any time UML Restricted and/or Confidential data is placed on a medium such as a CD, DVD, USB, or portable drive to facilitate a physical transfer, either entirely within UML or between UML and a 3rd party, that data must be encrypted. Archiving UML Restricted and/or Confidential data to a physical medium is not recommended, but is permitted if the data is encrypted. All archiving should be done electronically, so that it is stored in a controlled data center and backed up by Information Technology.

D. Software

Information Technology will install software that is capable of encrypting the entire hard drive on all identified UMass Lowell computers and electronic devices subject to this Policy. Users who require encryption software should contact IT Service Management to arrange installation of encryption software.

VI. RESPONSIBILITY

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

None

VIII. RELATED POLICIES, PROCEDURES AND ANNOUNCEMENTS

UMass Lowell Data Classification Policy, IT-5-106

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.