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

N/A

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 or contact the IT Service desk at 978-934-4357
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 listed in the appendix. 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

N/A

VIII. RELATED POLICIES, PROCEDURES AND ANNOUNCEMENTS

IT-5-106 UMass Lowell Data Classification Policy
IX. APPROVAL AND EFFECTIVE DATE

Approved:

_________________________________________ Date: _______________________
James Packard, ISO

_________________________________________ Date: _______________________
Michael Cipriano, CIO