I. POLICY STATEMENT

UMass Lowell appropriately secures its information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. This policy establishes the UMass Lowell strategies and responsibility for ensuring the confidentiality, integrity, and availability of the information assets that are accessed, managed, and/or controlled by the University. Members of the UMass Lowell community have individual and shared responsibilities to safeguard the information assets in accordance with federal, state, and local law, University policies, and agreements binding the University.

II. PURPOSE

The purpose of this policy is to provide a security framework that will ensure the protection of University information and resources from unauthorized access as well as ensuring the confidentiality, integrity and availability of Institutional Data stored, processed or transmitted by the University. Policies, procedures, and standards related to this Information Security Policy will be developed and published separately.

III. SCOPE

This Information Security Policy is applicable to all University faculty, staff, and students as well as third-party agents who are authorized to access Institutional Data including, but not limited to, contractors, temporary employees, and volunteers.

This policy refers to all UMass Lowell information resources and assets whether individually-controlled or shared, stand-alone, or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University. This includes networking devices, laptops, tablets, telephones, smart phones, wireless devices, personal computers, gaming systems, workstations/desktops, and any associated peripherals and software, regardless of whether it is used for administration, research, teaching or other purposes.

IV. DEFINITIONS

Agent - Any third-party that has been contracted by the University to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.
Authorization – the function of establishing and individual’s privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – refers to the level of assurance that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Institutional Data – refers to any data that is owned or licensed by the University.

Integrity – refers to the accuracy, completeness, and consistency of information.

Restricted Data – 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.

Unauthorized Access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling of information without proper authorization and legitimate business need.

University Asset – refers to data, information, system, computer, network device, document, contractual agreement, or any other component of the University infrastructure regardless of its medium or location, which is used by UMass Lowell employees to assist the University accomplish its mission.

V. PROCEDURES

In the absence of university policies, procedures, standards and guidelines mandates by either the University Information Security Office or the Chief Information Security Officer shall govern matters relating to information security.

A. Data Classification and Protection

In order to ensure that University data is properly protected, all information will be classified in accordance with the Data Classification Policy, IT-5-106. All University Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

B. User Training and Awareness

Effective information security requires a high level of participation from all members of the University and all must be well informed of their responsibilities. To facilitate this, information security awareness materials and training will be provided to the UMass Lowell community in accordance with the Security Awareness Policy, IT-5-111.

C. Physical and Environmental Security

Centralized computer facilities will be protected in physically secure locations with controlled access, in accordance to the IT Access Control Policy, IT-5-129. They will
also have appropriate environmental safeguards (i.e. HVAC, fire suppression) in accordance with IT specifications. Departmental computers housing UMass Lowell Sensitive or Public data may require physical and environmental security safeguards. All servers containing UMass Lowell Restricted data must be housed in an approved IT data center or a protected network.

D. Incident Response

Information security incidents have the potential to negatively impact members of the University community and to harm the University’s reputation. Therefore, it is important that all information security incidents are handled confidentially and appropriately. All information security incidents will be handled in accordance with the Security Breach and Response Policy, IT-5-118.

E. Risk Assessment

Security incidents are more likely to occur when there are unknown and unaddressed risks and vulnerabilities in information systems. Therefore, risk assessments will be conducted in accordance with the Information Security Risk Management Standard. In addition, the Information Security team will periodically perform vulnerability assessments, per the Vulnerability Management Policy, IT-5-116.

F. Network Security

All networking devices procured through, operated or contracted by the University will be configured in accordance with the IT Router and Switch Security Standard, the Firewall Standard, or the Wireless Policy, IT-5-132, depending on the type of device.

G. Computer Security

All workstations, desktops and laptops procured through, operated or contracted by the University will be configured in accordance with the Registration and Protection of Endpoints Standard, the Password Policy, IT-5-115, and the Antivirus Standard.

H. Server Security

All servers procured through, operated or contracted by the University will be configured in accordance with the Protection of Servers Standard, the Password Policy, IT-5-115, and the Antivirus Standard.

I. Data Encryption

All systems that store Restricted data will encrypt said data using appropriate encryption techniques, as defined within the Encryption Policy, IT-5-122, and according to the respective Technology Control Plans (TCP) for export controlled and restricted research.

J. Sanitation and Disposal of Information Resources

The surplus, transfer, trade-in, disposal of computers, or replacement of electronic storage media, and computer software can create information security risks for the University. This also includes equipment reassigned, or released, or no longer in use in the University. Failure to properly purge data in these circumstances may result in
Unauthorized access to University data, breach of software license agreements, and/or violation of state and federal data security and privacy laws. Refer to the Sanitation and Disposal of Information Resources Policy, IT-5-107.

K. Mobile Device Security

Every member of the UMass Lowell community who utilizes a mobile device (e.g. smartphones, tablets) is responsible for the university data stored on, processed or transmitted via that mobile device. All mobile computing and storage devices that access, store, process or transmit University Data, regardless of ownership, must be compliant with Mobile Device Security Standard.

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 ANOUNCEMENTS

| IT-5-106 | Data Classification Policy |
| IT-5-112 | Security Awareness Policy |
| IT-5-113 | IRB Data Security Policy |
| IT-5-115 | Password Policy |
| IT-5-122 | Encryption Policy |
| IT-5-107 | Sanitation and Disposal of Information Resources Policy |
| IT-5-132 | Wireless Policy |
| IT-5-118 | Security Breach and Response Policy [Reserved] |
| IT-5-116 | Vulnerability Management Policy [Reserved] |
| Protection of Endpoint Standard |
| Protection of Servers Standard |
| Log Management Standard |
| Mobile Device Security Standard |
| Information Security Plan |

| Effective As Of: | October 4, 2017 |
| Next Review Date: | October 4, 2018 |