University of Massachusetts Lowell

Policy Title:	Acceptable Use Policy
Policy Number:	IT-5-101
Effective As Of:	10/01/16
Next Review Date:	10/01/17
Responsible Office:	Information Technology
Responsible Position:	Information Security Officer

I. POLICY STATEMENT

UMass Lowell provides a wide variety of computing and networking resources to authorized members of the University community. These resources are intended to support the academic, research and business needs of the University community. Access to computers, computing systems, and networks owned by UMass Lowell is a privilege which imposes certain responsibilities and obligations on users.

Use of these resources is subject to University policies and regulations, and local, state, and federal laws. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources. Access to and use of these resources is issued on a temporary basis while the user is an active member of the University community (i.e. registered student, staff or faculty member, contractor, or university partner).

University-issued computer and network resources remain the property of the University at all times.

II. PURPOSE

The purpose of this policy is to outline the acceptable use of information technology resources at UMass Lowell and to promote the efficient, ethical, and lawful use of UMass Lowell's information technology resources. This policy addresses the responsibilities and obligations of users once access is granted. It is intended to protect students, faculty and staff, as well as the University and its resources.

III. SCOPE

This policy applies to all information technology resources, including personally-owned devices used for work-related purposes, at UMass Lowell and to each user of these resources. The resources include any and all University-owned or managed computer-related equipment, computer systems, access cards, and interconnecting networks, as well as all information contained therein. The user community consists of those persons and organizations which use, directly or indirectly, any of these resources.

IV. DEFINITIONS

N/A

V. PROCEDURES

A. Rights and Disclaimers

The University acknowledges the requirement to maintain user privacy and to avoid unnecessary interruption of user activities. To maintain a stable operating environment and to insure against unauthorized or improper use of those facilities, the University reserves the right, without notice, to inspect any data or file stored on the system(s) and/or data transmitted across the campus network consistent with the UMass Lowell Information Security Policy.

For reasons relating to compliance, security or legal proceedings (e.g. subpoenas) or in an emergency or in exceptional circumstances, the Office of the General Counsel or other appropriate authorizing agent of the University may authorize the reading or blocking of data. In particular, in the context of a litigation or an investigation, it may be necessary to access data with potentially relevant information.

B. Conditions of Use

a. UMass Lowell information technology resources are provided for University-related academic, business, and research activities and are to be used in a manner consistent with UMass Lowell policies, regulations, and procedures. Employees may use such resources for employment-related communications, including union-related communications, subject to the provisions of any applicable collective bargaining agreement.

b. Although UMass Lowell information technology resources are provided to employees for University-related purposes, the University recognizes that resources such as email and internet access may be appropriately and occasionally used by University employees for incidental personal use. Such personal use must be of a limited and reasonable nature, comply with all of the requirements of this policy, and not interfere with the performance of work duties, disrupt the workplace, or be otherwise inconsistent with the needs or functioning of the University.

c. Members of the UMass Lowell user community must use only those resources to which they have been specifically granted access by the University. The unauthorized use of resources is prohibited and may, in some cases, be violations of the law.

C. Prohibitive Actions

No user of information technology resources may take any of the following actions:

a. Use information technology resources in violation of UMass Lowell Information Security Policies.
b. Use information technology resources to gain unauthorized access to resources of this and/or other institutions, organizations, or individuals.
c. Violate any institutional polices or procedures or use information technology resources for unethical, illegal or criminal purposes.

d. Violate the privacy of co-workers, students, research subjects, alumni(ae) or donors.
e. Use of false or misleading information for the purpose of obtaining access to resources.
f. Authorize another person or organization to use your computer accounts. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not, for example, share your password with anyone else. You also must not provide anyone else's password, encrypted or otherwise, to anyone who is not authorized to have it.
g. Violate the rights of any person protected by copyright, trade secret, patent or other intellectual property or similar laws and regulations.
h. Use information resources in a manner that violates State or Federal Law or University policy (e.g. the use of resources for private gain).
i. Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, subroutine libraries, data and electronic mail) from system or public files or files of other users without prior authorization.
j. Use information technology resource irresponsibly or in a manner that needlessly affects the work of others. This includes transmitting or making accessible offensive, or harassing material; intentionally, recklessly or negligently damaging any system (i.e. by the introduction of any virus, worm, or Trojan-horse program); intentionally damaging or violating the privacy of information not belonging to you; or intentionally misusing or allowing misuse of system resources.
k. Use information technology resources or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material except when clearly required to do so in the course of your work.
l. Obstruct University business by consuming excessive amounts of network bandwidth and other system resources or by deliberately degrading the performance of a computer.
m. Intercept or monitor data not intended for the user unless specifically authorized by the Information Security Officer.
n. Attempt to avoid the user authentication or security of Systems and Endpoints.
o. Use University access cards in any manner to gain entrance to a restricted area. This includes providing an employee, student or non-university official (including vendor) with your personal access card to access a restricted area.
p. Use information technology resources to support or oppose a candidate for public office or a ballot measure in a manner contrary to state laws governing the political activities of public employees.

D. Required Actions

Each User of Information Resources must take the following actions:

a. Ensure that his/her account or password is properly used and is not transferred to or used by another individual.

b. Log off from a System or Endpoint after completing access at any location where such System or Endpoint may potentially have multiple users.
c. Ensure that Sensitive (Restricted) Data is protected with a password and encrypted while in transit or storage.
d. Report the loss or theft of any Endpoint or System containing Sensitive Data in accordance with the UMass Lowell Security Breach and Response Policy; and
e. Report any violation of these guidelines by another individual and any information relating to a flaw in or bypass of resource security, to the Information Security Officer, InfoSec@uml.edu.

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

N/A

VIII. RELATED POLICES, PRODEDURES AND ANNOUNCEMENTS

Information Security Policy, IT-5-111 (reserved)
Email Usage Policy, IT-5-108 (reserved)

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.