I. POLICY STATEMENT

UMass Lowell provides a wide variety of computing and networking resources to authorized members of the University community. Authorized members of the University community are expected to responsibly manage and use these resources in support of the academic, research and business needs of the University community. Access to and/or use of information technology resources, such as University owned or managed computer-related equipment, computer systems, access cards as well as, any information contained therein (“Information Technology Resources”) is a privilege which imposes certain responsibilities and obligations on its users. Use of Information Technology Resources is subject to University policies and regulations, as well as local, state, and federal laws.

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 Information Technology Resources. This policy addresses the responsibilities and obligations of authorized members of the University community. 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 at UMass Lowell and to each Authorized User of these resources. Only those members of the University community who have been granted current access to the Information Technology Resources by the University shall have access to and use of, the Information Technology Resources. An “Authorized User” is defined under Section IV, entitled “Definitions.” An Authorized User must comply with specific policies and guidelines governing their use, and act responsibly while using network resources. Access to and use of these information technology resources is issued on a temporary basis while the Authorized User is an active member of the University community.
IV. DEFINITIONS

Authorized User – In the context of this policy, an authorized user is a student who has been granted access to network resources including, but not limited to, the UMass Lowell network, Email, Student Information Systems, and Online Learning Management Systems.

V. PROCEDURES

A. Rights and Disclaimers

The University acknowledges its responsibility 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 transmitted across the campus network consistent with the UMass Lowell Information Security Policy, located on the UMass Lowell Policy website.

In response to compliance issues, security matters, legal proceedings (e.g. subpoenas), the Office of the General Counsel and the Information Security Officer may authorize access to student 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. Students are responsible for all traffic originating from their machine, regardless of whether they generated it or realize they have violated any specific policies. In most cases, unintentional violations will result in a temporary loss of network access pending the resolution of the problem and education of the student.

b. You must use only those resources to which the University has specifically granted you access. The unauthorized use of those resources is prohibited and may, in some cases, be violations of the law and the UMass Lowell Student Code of Conduct.

C. Prohibitive Actions

No student may take any of the following actions:

a. Use information resources in a manner that violates State and Federal Law or University policy.

b. Use information technology resources to gain unauthorized access to resources of this and/or other institutions, organizations, or individuals.

c. Use of false or misleading information for the purpose of obtaining access to resources.

d. Authorize another person or organization to use your computer account and/or student email account. 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 accounts 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.

e. Violate the rights of any person protected by copyright, trade secret, patent or other intellectual property or similar laws and regulations.

f. 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.
g. 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.

h. Obstruct University business by consuming excessive amounts of network bandwidth and other system resources or by deliberately degrading the performance of a computer.

i. Intercept or monitor university network traffic unless it is related to university coursework.

j. Attempt to avoid the user authentication or security of systems and endpoints.

k. Assign a static address to their computer while connected to the residential network.

l. Provide server-related services while on the residential network including, but are not limited to: mail, ftp, web, DHCP, DNS, game, and mIRC chat servers.

m. Illegally copy, distribute, share, download or upload copyrighted music, movies, software and games in violation of Federal Copyright laws. The University of Massachusetts Lowell is obligated by the Digital Millennium Copyright Act to take action on all notifications received regarding alleged copyright infringement.

D. Required Actions

Each student 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 their personal computer has installed operating system and application updates to address security vulnerabilities, as well as current antivirus software with current antivirus definition files.

It is the responsibility of all students to report any violation of these guidelines by another individual to the Information Security Officer at InfoSec@uml.edu.

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

Information Security Policy, IT-5-111 [Reserved]
Student Email Communication Policy, IT-5-119