I. POLICY STATEMENT

Installation, engineering, maintenance, and operation of wireless (WiFi) networks on any property owned or leased by the University, are the sole responsibility of UMass Lowell Information Technology. Any independent, unauthorized installed wireless communications equipment is prohibited, subject to removal from service without notice, and possible confiscation. Use of the University’s wireless network is subject to the same provisions as stated in the UMass Lowell Acceptable Use Policy.

II. PURPOSE

The purpose of this policy is to protect the University’s technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage the University’s public image. All users employing wireless methods of accessing University resources must adhere to University defined processes for doing so, using University-approved access points.

III. SCOPE

All University employees, students, consultants, contractors, and others who use the UMass Lowell network, including all personnel affiliated with third parties that may maintain an IT-approved wireless infrastructure device, must adhere to this policy. It applies to all wireless infrastructure devices that connect to the UMass Lowell network or reside at a University owned, leased or rented site that provides wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, tablets, and smartphones. This includes any form of wireless communications device capable of transmitting packet data.

IV. DEFINITIONS

Access Point: Any piece of equipment that allows wireless communication using transmitters and receivers to communicate. These devices act as hubs and allow communications to the campus Network.
**Baseline Level of Connection Service Quality**: The baseline level of connection service quality is determined by factors that can affect radio transmissions, such as distance from the access point, number of users sharing the bandwidth, state of the environment from which the transmission is taking place, and the presence of other devices that can cause interference. Acceptable throughput levels are determined by the scope of this policy.

**Coverage**: Coverage is the geographical area where a baseline level of wireless connection service quality is attainable.

**Interference**: Interference is the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or completely eliminate it depending on the strength of the signal.

**Privacy**: Privacy is the condition that is achieved when successfully maintaining the confidentiality of personal, student and/or employee information transmitted over a network.

**Security**: Security, as used in this policy, not only includes measures to protect electronic communication resources from unauthorized access, but also includes the preservation of resource availability and integrity.

**Wireless Infrastructure**: Refers to wireless access points, antennas, cabling, power, and Network hardware associated with the deployment of a wireless communications Network.

V. **PROCEDURES**

A. Wireless Standards Supported

- IEEE 802.11ac is the preferred wireless networking standard.
- IEEE 802.1X is the authentication standard. Additional security procedures may be applied as needed.
- WPA2 with AES encryption will be the only secure standard used.

To connect to the University’s wireless network, a computer or mobile device must be capable of using 802.1x encryption.

B. Acceptable Use

1. Use of the wireless network is subject to the same provisions as stated in the UMass Lowell Acceptable Use Policy.

C. Access-Authenticated Users

Role-based access to the wireless network shall be established using the user’s UMass Lowell Single-Sign-On (SSO) credentials. Services allowed through the wireless network will be identical to those for wired services. Authenticated role-based users will be limited to those same services they are permitted to access via wired network controls.
D. Access – eduroam Users

UMass Lowell supports eduroam, a secure, worldwide roaming wireless service developed for the international research and higher education community. Eduroam allows UMass Lowell employees and students to obtain free wireless connectivity at participating institutions around the world. This makes connecting to the Internet easy, convenient, and secure when visiting other campuses for conferences, research, or other reasons. Similarly, visitors from those participating institutions can easily get wireless access on the UMass Lowell campus by connecting to the eduroam network.

E. Access – Visitors and Guests

The guest network is available to anyone and is intended to allow guests/visitors to access standard Internet services, browse the web, etc. Services that require special protocols or ports (such as VPN applications) may not work on the guest network and are not supported. The guest network does not allow access to internal University resources. After registration via a guest portal, network connectivity is allowed for 12 hours.

F. Restrictions

a. All routers and wireless access points must be approved and centrally managed by the University’s Information Technology department. Non-approved installations of wireless equipment, or use of unauthorized equipment on campus premises, are strictly prohibited.

b. Information Technology reserves the right to disconnect, without notice, any access point connected to the network that places the University’s systems, data, or users at risk.

c. Any device or equipment found to be interfering with 802.11 access point broadcast frequencies (2.4GHz and 5GHz) and channels may be subject to relocation or removal.

d. Departments with research-related and/or clinical requirements to maintain a locally-managed wireless infrastructure are required to receive written permission from Information Technology to avoid possible interference with the UMass Lowell Wi-Fi network, unnecessary impact to the wired network, and to minimize security risks.

G. Additional Security Measures

a. All approved wireless access points / base stations are subject to periodic
penetration tests and audits.

b. All wireless access users agree to immediately report any incident or suspected incidents of unauthorized access point installation to Information Technology.

c. All wireless clients and devices shall be required to be fully patched and have university-approved antivirus software installed and maintained. University employees may obtain antivirus software by visiting the Information Technology website.

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

VIII. RELATED POLICIES, PROCEDURES AND ANNOUNCEMENTS

IT-5-101 UMass Lowell Acceptable Use Policy

IX. APPROVAL AND EFFECTIVE DATE

Approved:

________________________________________ Date: _____________

James Packard, ISO

________________________________________ Date: _____________

Michael Cipriano, CIO