60-5 Campus Wireless Network

60-5-1 Purpose • 60-5-2 Policy • 60-5-3 Administration • 60-5-4 Definitions • 60-5-5 Responsibility for Network • 60-5-6 Access and Use • 60-5-7 Restrictions • 60-5-8 Enforcement

1. **Purpose.** The purpose of this policy and procedures is to assign responsibility for the design, deployment, management, coordination and operation of the Eastern New Mexico University System (the System) wireless network infrastructure and to monitor the use of frequencies that can, do or have the potential to interfere with the performance and/or operation of the wireless network.

2. **Policy.** The policies established in support of the purposes stated above are as follows.

   A. The wireless connections provided by the System shall be used for business purposes and by authorized users only.

   B. In addition to the policies and procedures stated here, the use of wireless connections on ENMU-Portales, ENMU-Roswell and ENMU-Ruidoso are subject to the following:

      (1) The ENMU System's policy on computer use, found in AGP&P, 60-1;

      (2) Procedures established for inventory control and

      (3) Any additional guidelines for the use of wireless network resources issued by System's Information Technology Services (ITS).

The foregoing purposes and policies are implemented by the following.

Procedures

3. **Administration.** These policies and procedures are administered by ITS, with oversight by the System chief information officer (CIO).

4. **Definitions.**

   A. "Wireless network access" means a local area network (LAN) or single computer not connected to a network by wires but through the use of wireless radio technologies.

   B. "Wireless access point" means a device connected to the wired LAN that receives and transmits signals to wireless devices or computers. This device must also be connected to the wired LAN if connections to external networks are required.

5. **Responsibility for Network.** ITS shall be responsible for the wireless network. The scope of this responsibility includes but is not limited to the following: associated standards, system deployment and management, authentication, security and access points of the System.

6. **Access and Use.** ITS shall offer a standard wireless deployment plan which is expected to meet the network access needs of most departments, student groups, individuals and/or campus organizations. Departments shall contact ITS for the approval of the purchase, implementation and maintenance of alternate wireless network deployment. It is also the responsibility of the user to notify ITS regarding the coordination and relocation of any wireless equipment or to report any problems with the wireless network connection or an access point.

7. Restrictions. Departments, student groups, organizations or individuals of the System shall not install or deploy any device or service anywhere on System property (including student housing) that interferes or has the potential to interfere with the System wireless network managed by ITS without coordination and approval from ITS. This includes devices that are not attached to the network but may interfere with wireless access points managed by ITS.

8. Enforcement. To ensure the security and cost effectiveness of the System wireless network, ITS may take the following actions against those not complying with this policy.

A. ITS is authorized to disconnect and remove, without warning, any unauthorized wireless access point or another device it discovers attached to the network.

B. ITS is authorized to direct a department, student group, organization or individual to remove or disable any device not previously approved by ITS that interferes with the operation and/or performance of the network.

Approved by the Board of Regents on May 12, 2006.
Amended policy approved by the Board of Regents on April 25, 2014.
Amendments approved by the Board of Regents on March 29, 2019