Wireless Standards

ITS Standards

The University at Albany network is a community resource that supports the academic, research and business functions of the institution. The wireless infrastructure, UAlbany WiFi, is based on the IEEE 802.11 b/g/n/ac standard.* All devices using the campus network are subject to the terms and conditions of UAlbany's Connecting Devices to the University Network policy. This document specifies the requirements for accessing wireless services in compliance with that policy.

Wireless environments tend to be less secure than their wired counterparts and are prone to interference from competing equipment, physical infrastructure and other impediments. Given this, wireless service should not be viewed as a replacement of wired connectivity, nor should critical applications rely on a wireless network. These standards were developed to maximize the availability of wireless access to authorized users, provide information about the service, and establish safeguards to minimize the vulnerabilities typically associated with wireless networks.

Standards for Use:

- All users must connect using UAlbanyWiFi or Eduroam SSID.
- All users must register their wireless devices upon connecting to the network and identify themselves as a member of the University community.
- Guest access is available for unsecured, unencrypted access to the Internet. Guest IDs are available to faculty/staff in MyUAlbany. Select "UAlbany Guest Wireless Access" from the Self Service panel of the portal.

Standards for Equipment:

- All wireless access points must be authorized by Information Technology Services and comply with industry standards and University policies. Unauthorized access points are strictly prohibited and subject to removal without notice.
- All wireless access must be encrypted and secure with the exception of sponsored guest access.
- The University establishes compliance specifications for hardware and software.

Responsibilities of Information Technology Services:

Information Technology Services is ultimately responsible for the University network, including its wireless infrastructure. The CIO or designee has the authority to enforce these standards and to ensure that wireless technology is deployed in a safe and secure manner. The responsibilities of the CIO or designee include the following:

- Creating, maintaining and updating wireless use and security standards
- Maintaining active, accurate registration of all wireless networks and wireless access points on campus
- Approving departmental installations of wireless network and access points
- Managing and deploying wireless connectivity in common areas and assisting departments with the development, management and deployment of approved wireless networks
- Monitoring performance and security of all wireless networks
- Maintaining statistics regarding unauthorized access to the campus network
- Resolve problems arising from any wireless device that interferes with other equipment
- Evaluating wireless network technology enhancements

Companion Documents:

Connecting Devices to the University Network
Responsible Use of Information Technology Policy
Information Security Policy

Need more help? Contact the ITS Service Desk.