Wireless

Effective: March 31, 2004
Updated: April 18, 2025
Contact: Information Technology Services (ITS)

Contents

Introduction

Iowa State University's wireless network enables mobile computing and provides network services in many situations where wired network connectivity is not available.

The purpose of the wireless policy and related standards and guidelines is to assure students, faculty, and staff access to a reliable, robust, and integrated wireless network and to increase security of the campus wireless network to the extent possible.

This document provides policies, standards, and guidelines for best practice as they relate to providing and using Iowa State University's wireless network. Specifically, the policy identifies user and service provider responsibilities, lists the industry wireless standards supported on campus, addresses frequency management, stresses the importance of security, and provides guidelines and best practices to improve security.

Policy Statement

1. Responsibility and Enforcement

The Information Technology Services (ITS) Network team is solely responsible for implementation of wireless technology, enforcing campus network standards, and has the authority to resolve frequency interference issues. All users connecting to the campus network will gain access through their Net-ID which determines the identity of and authenticates the user.

The addition of new wireless access points on the University network must be coordinated and approved by the ITS Network team. Wireless performance is impacted by architectural features, building materials, and furnishings of a workspace. Construction renovation projects must be coordinated with ITS and include funding for additional wireless equipment as required to optimize performance and serviceability of impacted systems.

Any devices either not part of or that cause significant Radio Frequency (RF) interference to the University wireless network will be considered a “rogue” access point or device. ITS will pursue all reasonable efforts to contact the owner of the rogue device, and if necessary, may disable or disconnect it from the University network.

2. Standards

Iowa State University has adopted the following approved IEEE (Institute of Electrical and Electronics Engineers, Inc.) standard protocols for wireless networking. This list does not cover all the possible standards nor does it restrict the standards that the ITS Network team may use. New standards may be adopted or old standards may be deprecated as needed to ensure a dependable and robust wireless solution:

- **IEEE 802.11g** provides up to 54 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency. 802.11g is supported in all public spaces although the access points do not solely broadcast 802.11g data rates.
- **IEEE 802.11n** provides up to 144 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency, and up to 300Mbps of shared bandwidth using the 5GHz radio frequency. 802.11n client devices are supported in all public spaces, although the access points do not solely broadcast 802.11n data rates.
- **IEEE 802.11ac** provides up to 433Mbps of shared bandwidth using the 5GHz radio frequency. 802.11ac client devices are supported in all public spaces.
- **IEEE 802.11ax** provides up to 600Mbps of shared bandwidth per access point using 2.4GHz, 5GHz, and 6GHz frequencies. 802.11ax client devices are supported and are backwards compatible with 802.11ac access points available in all public areas.
- **IEEE 802.11be** provides multi-gigabit of shared bandwidth per access point using 2.4GHz, 5GHz, and 6GHz frequencies. 802.11be client devices are supported and are backwards compatible with 802.11ac access points available in all public areas.

3. Frequency Use

The 2.4 GHz, 5GHz, and 6GHz radio frequencies are unlicensed shared spectrum bands which are used by 802.11g, 802.11n, 802.11ac, 802.11ax and 802.11be access points. As a result, there are a limited number of channels within each spectrum that can be utilized. Access points and other communications devices or appliances can interfere with each other if not administered or deployed properly. Microwave ovens, personal mobile hotspots and other wireless peripherals are prominent examples. The ITS Network Infrastructure team will manage the shared use of unlicensed radio frequencies for the campus community and has authority to resolve interference issues.

4. User Provided Equipment

Users are responsible for acquiring wireless clients or devices that are compatible with the campus wireless network. Detailed specifications for these devices can be found in the Desktop Computers Standards. Due to the wide variances in manufacturing and device requirements, ITS cannot guarantee or support all wireless devices on the network. It is suggested that users vet their equipment prior to purchase by contacting ITS to ensure compatibility and avoid connectivity issues.

5. Security

Wireless networks are not as secure as wired networks. ITS recommends connecting to “eduroam” for the most secure wireless connection. ITS is responsible for establishing security policies for wireless communications based on current best practices. All wireless network installations must comply with established security policies including campus-wide IP (Internet Protocol) addressing and DHCP (Dynamic Host Configuration Protocol) services.

6. Experimentation

ITS continually tests new and emerging wireless technologies. Departments and colleges may test new technologies, but may not implement technologies that compete or interfere with the campus wireless network. Departments must notify ITS of any new wireless technology trials, particularly those that may interfere with frequencies in use by the campus wireless solution.

7. Service Spaces

7.1. Public Spaces

ITS Network Infrastructure team is responsible for providing and upgrading wireless service in public spaces for a robust, seamless, and integrated wireless network.

- Public areas include but are not limited to areas such as atriums, general-purpose classrooms, and outdoor areas.
- 802.11g, 802.11n, 802.11ac, 802.11ax, and 802.11be are supported in public spaces.
- ITS maintains a list prioritizing public areas for central funding. Departments may request ITS wireless services in public areas not yet covered by central funding.

7.2. Residence Hall Spaces

ITS Network Infrastructure team is responsible for providing and maintaining wireless networking services in Residence Hall spaces for a robust, seamless, and integrated wireless network.

- Residence Hall areas include dormitory rooms, apartments, dens, study areas, dining halls, and community centers.
- 802.11g, 802.11n, 802.11ac, 802.11ax, and 802.11be are supported in residence hall spaces.
- Installation of wireless routers or access points not supported by ITS in residence halls spaces violates the Department of Residence housing contract and may result in fines or cancellation.
- Some Residence Hall locations are excluded from ITS networking services. These locations are determined by agreement between ITS and the Division of Student Affairs.

7.3. Department Spaces

Departments have two options for extending wireless service to locally controlled areas defined as not public or residence spaces.

ITS Wireless Service

Wireless service (including access points, technical support, software and hardware upgrades) is available from ITS for extending wireless networking beyond the public areas into departmental spaces. The ITS Network Infrastructure team division will provide engineering for optimal placement of access points and identify other devices operating in the same frequency range. They will also make a determination of the appropriate source of power, i.e. AC power at the device or power over communication lines from the Communications closet. ITS wireless service includes software and hardware maintenance and technology upgrades.

Self-supported Wireless Services

If the ITS wireless service will not be sufficient for the needs of the department, a written request may be submitted to the CIO requesting authorization to place self-supported wireless services. Departments can provide access points within buildings in locally controlled areas. Any access point departmentally purchased and/or connected to the campus network must be coordinated and approved by ITS and meet the campus wireless standards outlined in this policy. Service Set Identifiers (SSIDs) must be sufficiently unique from centrally managed SSIDs so as to not cause confusion of which department owns and operates that SSID. Departmentally owned access points are responsible for the data and network traffic that traverses through the access point and appropriate access control and security configuration, as well as the regular maintenance, software updates, and replacement.

7.4. Inter-building and Off-campus Spaces

ITS is solely responsible for providing wireless networking between campus buildings and to off-campus locations. Departments are not permitted to provide inter-building or wide-area wireless services, "wireless bridging", or any form of "point to point" wireless connectivity for the purpose of wirelessly connecting two buildings.

8. Guidelines for Best Practice

Wireless networks inherently have greater risks than wired networks because wireless transmissions occur on unlicensed radio frequencies. Consequently, it is difficult to know who or what devices are connected and listening. Security of wireless networking in the open culture of a university network requires the best efforts of both the wireless service provider(s) and wireless users. Following these best practices will not guarantee security but may reduce the risks.

8.1 Non-ITS Wireless Service Providers

- Must not interfere with ITS provided wireless network services including avoiding nearby public space access point channel frequencies.
- Use directional antennas and other methods to reduce propagation of radio waves outside the perimeter of the locally controlled area.
- Must not use Service Set Identifiers (SSIDs) similar to ITS operated wireless network including but not limited to IASTATE, IASTATE-guest, and eduroam or use any SSID with ISU branded designations.
- Outdoor access points must only be installed by ITS.
- Access points installed in locally controlled areas should be securely mounted or in places not easily accessible by the public.
- Connect access points to an Ethernet jack or Ethernet switch.
- Use 1Gbps Ethernet where available when connecting access points to the campus network.
- When installing an access point, change the default password immediately and change access point password at least annually.
- Protect wireless network with a PSK (Pre-shared Key) with at a minimum WPA2 encryption.
- Mac address access lists can also be used to control access through wireless access points.
- Configure access points in bridging mode to the wired network. NAT (Network Address Translation) is not allowed.
- Access points must not provide their own DHCP IP addresses. Disable any DHCP functions built into an access point.
- Disable 802.11, 802.11b, or 802.11a data rates.

8.2. Wireless Network Users

- Wireless should only be used for mobile computing. Anytime wired access is available, it should be used for increased security and performance.

- Wireless services are offered at “best effort”, and no guarantees are made about the service level or performance.
- To ensure that communications are secure, wireless users should use the “eduroam” wireless network and/or VPN (Virtual Private Network) services.
- All campus network users must register with NetReg to obtain an IP address while using the “IASTATE” wireless network. The purpose of NetReg is for authentication of users and tracking users and devices, not to limit access.
- Guests to Iowa State University campus should use the “IASTATE-Guest” wireless network.
- Wireless users on campus must use DHCP, static IP addresses are not supported for wireless clients.