



Wireless Computing Guidelines

Technology Guideline

Purpose

Wireless Ethernet systems and interface cards will be deployed at UNI to support both administrative and academic applications. This policy guides such deployments. Policies and guidelines for deployment of these systems are essential to:

- Prevent interference among uses of the wireless radio spectrum.
- Safeguard security of campus network systems.
- Ensure that a baseline level of connection service quality is provided to a diverse user community.

Scope

Information Technology Service Network Services (ITS NS) is responsible for providing a functional yet secure and reliable campus wireless network. This will be accomplished by the use of campus-wide network standards and policies and limiting access to data network connections that do not conform to this document. Electronic communications is changing rapidly both in terms of technology and application and additional policy questions will surely arise in this area.

Frequencies: ITS NS is responsible for the management of all unlicensed radio frequencies used for wireless data communications, in order to prevent interference, safeguard University resources, and ensure service.

Network Reliability: Wireless network reliability is determined by both the level of user congestion (traffic loads) and service availability (interference and coverage). This policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum. ITS NS approaches the shared use of the wireless radio frequencies in the same way that it manages the shared use of the wired network. ITS NS will not actively monitor use of the radio frequency bands for potential interfering devices. ITS NS will respond to reports of specific devices that are suspected of causing interference and disrupting the campus network and will work towards a resolution.

Security: Due to the shared, broadcast nature of wireless transmissions, the security surrounding password and data transmission are serious concerns that must be addressed. Wireless devices utilizing the campus infrastructure must meet certain standards to ensure only authorized and authenticated users connect to the campus network and that institutional data is not exposed to unauthorized viewers. Support: ITS Network Services will provide installation, configuration and management services for all wireless access points connected to the UNI wireless infrastructure. In order to reduce support costs ITS will standardize on selected products that meet the performance, reliability, and management criteria. ITS User Service Computer Consulting Center will provide support for connectivity issues.

Interference: Wireless networking equipment is a technology that uses unlicensed radio frequency bands to create small local area network cells. The success of any wide deployment wireless networking requires that all equipment that operate in the frequency spectrum be carefully installed, configured and monitored to avoid physical and logical interference among networked systems and other equipment.

Suitability: Wireless networks are not a substitute for wired network connections. Wireless should be viewed as an augmentation to the wired network that will extend the network for general access to common and transient areas. As such,

priority for wireless communications should be to mobile computing needs (i.e. personal laptop, handheld, palm pilots, etc.) and to spaces that do not lend themselves to wired computing (auditorium, mobile labs, open spaces, etc.)

Policy

Frequencies: This policy governs the use of the unlicensed 2.4GHz and 5.0GHz radio frequency (RF) bands by the University of Northern Iowa.

Suitability: As an extension of the campus wired network, priority for wireless communications should be to mobile computing needs and to spaces that do not lend themselves to wired computing.

Responsibility for Wireless Access Points: Campus responsibility for electronic communication resources resides with Information Technology Services Network Services. ITS NS must approve all installations of wireless access points used on the campus.

- Wireless equipment and users must follow general communications policies:
- Wireless services are subject to the same rules and policies that govern other electronic communications services at UNI.
- Interference or disruption of other authorized communications is a violation of policy.
- Unauthorized interception of wireless data is a violation of policy.
- Wireless access points must meet all applicable rules of regulatory agencies, such as, the Federal Communications Commission .
- Wireless access points will be installed so as to minimize interference with other RF activities.
- ITS NS shall approve installation and manage all wireless access points.
- Only hardware approved by ITS NS shall be used for wireless access.

Funding for Wireless Access Points: ITS will be responsible for the purchase of wireless access points for common areas of the campus and will purchase this equipment when funds are available. Such locations include, but are not limited to: Public access and general conference room areas; Open seating areas where members of the community may sit and work, including space where people meet/gather/study that are not served by instructional or administrative access points.

Departments will have fiscal responsibility for wireless access points serving instructional and administrative uses. This would include coverage of classrooms, labs, offices, conference rooms, staff lounges and work areas. ITS will match funding for the purchase of access points. Matched funding is not available for the purchase of wireless network interface cards (NIC).

Installation: All new installations must be completed so as to minimize interference with existing access point coverage areas and to ensure baseline levels of connection service quality. Installation of antennas must comply with all federal and state regulations and must be consistent with health, building, and fire codes.

Interference: Use of wireless technology should be evaluated based on the suitability of the application in the space to be served. In the event that a wireless device interferes with other wireless access points or equipment, ITS NS shall initiate a meeting with affected parties to resolve interference. The PPCIT shall have ultimate authority to make determinations regarding conflicts in the use of wireless frequencies.

ITS NS reserves the right to restrict the use of any wireless device in situations where interference results in service interruption until an appropriate resolution is found.

- Security: General access to the network infrastructure, including wireless infrastructure, will be limited to individuals authorized to use campus resources. All users shall be authenticated.

- UNI wireless infrastructure will be limited to UNI faculty, staff, currently enrolled students, and approved affiliates/guests.
- All uses of the UNI wireless infrastructure will require authentication.
- ITS managed username/passphrase combinations will be the primary authentication method.
- MAC address authorization may be used for specialized networks where Internet or other access not requiring use of UNI managed username/passphrase is justified.
- All access through the wireless infrastructure using ITS managed username & passphrase combinations must be encrypted.
- ITS will provide a centralized approach to passphrase and data protection. It is expected that the technology for passphrase and data protection may change over time. Users of the UNI wireless infrastructure will be expected to upgrade local client hardware and software when changes to security solutions are made.
- ITS will provide centralized procedures to ensure that wireless devices connected to the network are free of viruses/worms, etc.
- In public areas, access points will be mounted in a manner that will deter theft or direct connection to data port.

Responsibility

Policy and Planning Committee for Information Technology (PPCIT)

- Review wireless communications policy standards.
- Resolve communication interference conflicts.

ITS NS

- Maintain a registration of all wireless networks and access points on campus.
- Create, maintain and update wireless security standards.
- Resolve wireless communication interference problems.
- Manage and deploy all wireless communications access points.
- Approve campus wireless communication hardware and software.
- Inform wireless users of security and privacy policies & procedures related to the use of wireless communications in common areas.
- Monitor performance and security of all wireless networks and maintain network statistics as required to prevent unauthorized access to the campus network.
- Monitor the development of wireless network technologies, evaluate wireless network technology enhancements and, as appropriate, incorporate new wireless network technologies within UNI.

Campus Units

- Adhere to Wireless Communications Policy.
- Share in funding for access points to serve classrooms, offices, etc.
- Inform wireless users of security, privacy policies and procedures related to the use of wireless communications.
- Ensure that use is limited to authorized users of UNI wireless infrastructure

Revised February 9, 2004. Implemented by PPCIT November 20, 2003

Source URL: <http://www.uni.edu/its/policies/wireless-computing-guidelines>