Wireless Communications Policy

its.fsu.edu/About-Us/IT-Policies-Guidelines/Wireless-Communications-Policy

Purpose

This section sets forth the policies for using wireless technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio spectrum. This policy describes how wireless technologies are to be deployed, administered and supported at Florida State University (FSU). This document specifically addresses wireless communications and the resolution of interference issues that might arise during use of specific frequencies. The policy couples the desire for campus constituencies to deploy wireless technologies with a central administrative desire to ensure that all constituents be assured of deploying such systems with an acceptable level of service quality and security.

Wireless Ethernet systems and interface cards will be deployed at FSU 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 between different departmental implementations and other uses of the wireless spectrum.
- Safeguard security of campus Network systems.
- Ensure that a baseline level of connection service quality is provided to a diverse user community.

This policy helps define a level of service that the campus community should assume as part of the campus wireless infrastructure.

Scope of the Policy

FSU is responsible for providing a secure and reliable campus Network. Information Technology Services (ITS) shall be responsible for providing services of the scope of this policy. 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.

This policy governs use of Electronic Communications Resources. Electronic communications is changing rapidly both in terms of technology and application and additional policy questions will surely arise in this area. This policy is to deal with known concerns and therefore does not constitute a comprehensive policy statement, but rather a beginning.

Frequencies: FSU is sole owner of the unlicensed frequencies on campus, to prevent interference, safeguard University resources, and ensure service.

Network Reliability: Network reliability is determined by both the level of user congestion (traffic loads) and service availability (interference and coverage). In efforts to provide an acceptable level of reliability, this policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum. The campus approaches the shared use of the wireless radio frequencies in the same way that it manages the shared use of the wired Network. While ITS does not actively monitor use of the airspace for potential interfering devices, we will respond to reports of specific devices that are suspected of causing interference and disrupting the campus Network. Where interference between the campus Network and other devices cannot be resolved, ITS reserves the right to restrict the use of all wireless devices.

Security: The maintenance of the security and integrity of the campus Network requires adequate means of ensuring that only authorized users are able to use the Network. Wireless devices utilizing the campus wired infrastructure must meet certain standards to ensure only authorized and authenticated users connect to the campus Network and that institutional data used by campus users and systems not be exposed to unauthorized

viewers.

Support: This policy includes the responsibilities of campus units and centralized support organizations for the planning, deployment, management and development of wireless network equipment and services. ITS is responsible for providing service to departments wanting to install data Networks.

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.

Policy

Responsibility for Wireless Access Points: Campus responsibility for electronic communication resources resides with FSU and/or ITS. FSU and/or ITS must approve 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 FSU.
- Abuse or interference with other activities is a violation of acceptable use.
- Interference or disruption of other authorized communications or unauthorized interception of other traffic is a violation of policy.
- Wireless access points must meet all applicable rules of regulatory agencies, such as the:
  - Federal Communications Commission
  - Public Utilities Commission

- Wireless access points must be installed so as to minimize interference with other RF activities particularly as described below.
- Only hardware and software approved by ITS shall be used for wireless access.
- Deployment and management of wireless access points in common areas of the campus is the

responsibility of ITS. Such locations include, but are not limited to:

- Public access area and general conference room areas
- Open seating areas where members of the community may sit and work, including space where people meet/gather/study
- Cafes
- Lounges
- General Lecture halls

Department heads are responsible for the installation of wireless access points within campus buildings used by the department, following ITS recommendations. Where more than one department share a common building, the Department heads may jointly share responsibility for wireless access points in that building or request ITS to take responsibility in these areas.

Department heads shall register any deployment of wireless access points with ITS. This registration shall provide information requested by the wireless overseeing committee.

Installation of Access Points will be the responsibility of the individual department, but must comply with rules and regulations of the University as implemented by the overseeing committee and enforced by ITS. I.E., all installations must not interfere with existing installations and cooperation must be awarded to ensure baseline levels of connection service quality. Installation of antennas must comply with all federal and state regulations for antennas. The installation of access points and bridging devices must be consistent with health, building, and fire codes.

Security: General access to the Network infrastructure, including wireless infrastructure, will be limited to individuals authorized to use campus and Internet resources. Users of campus and Internet resources shall be authenticated.

- Physical Security of wireless access points will be maintained to protect the access point from theft or access to the data port.
- Password and data protection is the responsibility of the application. The wireless infrastructure will not provide specialized encryption or authentication that should be relied on by applications. In particular, no application should rely on IP address based security or reusable clear text passwords. It is expected instead that service machines will expect/require their own general or applications authentication, authorization and encryption mechanisms to be used by clients entering from any unprotected Network.
- Access points or the security gateway shall provide user authentication and/or authorization to the Network before access shall be given.

Interference: Wireless networking equipment is a technology that uses the unlicensed frequency bands to create small local area Network cells. These cells can be further linked together over an underlying wired Network to create an extended wireless network covering whole buildings or wider areas. The success of any wide deployment wireless network requires that all equipment that operates in the frequency spectrum to be carefully installed, configured and monitored to avoid physical and logical interference between components of different Network segments and other equipment. In the event that a wireless device interferes with other equipment, the University shall resolve the interference as determined by this policy and enforced by ITS.

The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list:

- Public Access
- Administration
- Instruction
- Research

- Personal

Suitability: Wireless Networks are not a substitute for wired Network connections. Wireless should be viewed as an augmentation to the wired Network to extend the Network for general access to common and transient areas.

- Wireless is appropriate for "common areas" where students, staff, and faculty gather. Common areas most appropriate for wireless use include but not limited to, instructional labs, public areas, and research labs.
- Wireless Network is most applicable for uses such as email and web browsing. Unless using encrypted protocols, wireless devices should not be used for connecting to campus business systems such as human resources, payroll, student information, financial information systems, or other systems that contain sensitive information or are critical to the mission of the University unless a Virtual Private Network (VPN) client is used.
- Wireless access points provide a shared bandwidth. As the number of users increase the available bandwidth per user diminishes. Before deploying a wireless network in common areas, the advice of the University overseeing committee and/or ITS should be sought regarding the ratio of users to access point.
- New plans for buildings and gathering areas should consider the need for and use of wireless network, similar to the planning done currently for wired Network.
- Users of wireless should consider all unencrypted communications over the Network as insecure and available and all content as clear text.

Responsibility

Overseeing Committee

- Creating, maintaining and updating wireless communications policy standards.
- Creating, maintaining and updating wireless communication Network security policies.
- Resolving communication interference problems if political problems occur.
- Appointing new technology designee.

ITS

- Maintaining a registration of all wireless Networks and access points on campus.
- Creating, maintaining and updating wireless communications wireless security standards.
- Resolving wireless communication interference problems.
- Appointing new technology designee.
- Managing and deploying wireless communication systems in common areas of the campus.
- Approving wireless communication hardware and software used by campus departments.
- Approving departmental installations of wireless communication systems/access points.
- Informing wireless users of security and privacy policies & procedures related to the use of wireless communications in common areas.
- Providing assistance to campus units for the development, management and deployment of wireless Networks.
- Monitoring performance and security of all wireless Networks within common areas and maintaining Network statistics as required to prevent unauthorized access to the campus Network.
- Monitoring the development of wireless network technologies, evaluating wireless network technology enhancements and, as appropriate, incorporating new wireless network technologies within FSU.

Campus Units

- Adhering to Wireless Communications Policy.

- Managing access points within departmental space and assuring proper security is implemented in accordance to this policy.

- Registering wireless access point hardware, software, and deployment information to ITS and Overseeing committee.

- Informing wireless users of security, privacy policies and procedures related to the use of wireless communications.

- Monitoring performance and security of all departmental wireless equipment to prevent unauthorized access to campus Network.

- Provide following "reference" information:* Department name

    - Contact name

    - Contact number

    - Contact e-mail address

    - Equipment description (i.e., manufacturer, model number, firmware version, software versions)

    - Protocol information

    - System configuration

    - Planned placement & coverage areas

    - Number of channels

    - Output power