**Wireless Network 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 ***<Company Name>***. This document specifically addresses wireless communications and the resolution of interference issues that might arise during use of specific frequencies.

Wireless Ethernet systems and interface cards will be deployed at ***<Company Name>*** to support all the 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 organization’s 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 organization should assume as part of its wireless infrastructure.

* **Scope**
* ***<Company Name>*** is responsible for providing a secure and reliable 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 organizational 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:** ***<Company Name>’s*** management is sole owner of the unlicensed frequencies in the organization’s premises, to prevent interference, safeguard 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 organization 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 for potential interfering devices, we will respond to reports of specific devices that are suspected of causing interference and disrupting the organization’s network. Where interference between the organization’s 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 network requires adequate means of ensuring that only authorized users are able to use the network. Wireless devices utilizing the ***<Company Name>’s*** wired infrastructure must meet certain standards to ensure only authorized and authenticated users connect to the network and that the data used by employees should not be exposed to unauthorized viewers.
* **Support:** This policy includes the responsibility of organization 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.
* **Policy**

**Responsibility for Wireless Access Points:** Organization’s responsibility for electronic communication resources resides with the management. The management must approve installations of wireless access points used in the premises.

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 ***<Company Name>***
* 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 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

Administrators are responsible for the installation of wireless access points within the organization’s buildings.

Installation of Access Points must comply with rules and regulations of the ***<Company Name>*** as implemented by the overseeing committee and enforced by ITS. 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 only to the employees. 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 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 organization 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 employees 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 that contain sensitive information or are critical to the mission of the organization 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 organization 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.

**Source:** <http://its.fsu.edu/About-Us/IT-Policies-Guidelines/Wireless-Communications-Policy>