

**University of Utah**  
**Office of Information Technology**  
**Wireless Network Policy**

January 11, 2002

I. PURPOSE

The effective management of information technology resources is crucially important to the success of the academic, research, patient care and public service missions of the University of Utah. Because of the inherent nature of wireless communication, wireless networks require increased cooperation and coordination between campus entities to maximize the technology's benefits to the students, faculty, and staff of the University, to allow connection to wireless networks in different campus buildings, and eventually, to facilitate the ability to roam from building to building without losing network connectivity.

This document sets forth the policies for using wireless technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio frequency spectrum in a distributed campus network environment. This policy expands the Office of Information Technology Network Connection Policy by including specific direction regarding wireless communications and the resolution of issues that may arise.

This policy is subject to change as new technologies and processes emerge.

II. REFERENCES

Network Monitoring Policy

Network Connection Policy

ISO Minimal Security Requirements and Practices

Policy and Procedures 1-15: Information Resources Policy  
<http://www.admin.utah.edu/ppmanual/1/1-15.html>

Policy and Procedures 1-12: University Institutional Data Management Policy  
<http://www.admin.utah.edu/ppmanual/1/1-12.html>

III. DEFINITIONS

- A. Wireless Network means local area network technology that uses radio frequency spectrum to connect computing devices to college, department, and division wired networks and may connect to the Campus Network Backbone and the Internet.
- B. Access Point means electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a LAN, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the campus network backbone.
- C. Wireless Infrastructure means wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.
- D. Coverage means the geographical area where a baseline level of wireless connection service quality is attainable.

- E. Interference means the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
- F. Privacy means the condition that provides for the confidentiality of personal, student, faculty and staff communications, and institutional and patient data transmitted over a wireless network.
- G. Client hardware/software means the electronic equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide a LAN interface to a wireless network.

#### IV. SCOPE

This policy applies to all wireless network devices utilizing University of Utah IP space (including private IP space within University networks) and all users of such devices, and governs all wireless connections to the campus network backbone, frequency allocation, network assignment, registration in the Domain Name System, and services provided over wireless connections to the campus network backbone to colleges, departments, or divisions of the University of Utah.

#### V. AUTHORITY

- A. This policy is under the authority and oversight of the Information Technology/e-Commerce Executive Committee (ITeC).
- B. Technical review of this document is under the direction and authority of the Information Technology Advisory Committee (ITAC) of the University of Utah.

#### VI. POLICY

- A. Wireless equipment and users must follow all network connection policies as set forth in the Office of Information Technology Network Connection Policy. All provisions of the University IT Security and ISO Minimal Security Requirements and Practices apply to this policy.
- B. All acceptable use provisions of Paragraph V.C, Individual Responsibility, PPM 1-15 Information Resources Policy apply to wireless network services. Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited.
- C. Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.
- D. Deployment and management of wireless access points in areas not controlled by University college's, departments, or divisions is the responsibility of the University NetCom department under the direction of the Associate Academic Vice President for Information Technology, the Office of Information technology and the Information Technology / e-Commerce Executive Committee.
- E. Deans, department chairs, and directors of academic units are responsible for wireless access points within campus buildings used by the college, division or department. Where more than one organization share a common building, the deans or department heads may share responsibility for wireless access points in that building, or may designate a specific dean or department head to take responsibility for the wireless access points in that building.
- F. University colleges, departments, or divisions must register for the use of radio frequency spectrum with NetCom, prior to implementation of wireless networks.
- G. The location of all wireless access points must be registered with the University's NetCom department. This may be accomplished by sending e-mail to [apalloc@utah.edu](mailto:apalloc@utah.edu).

- H. A "Point of Contact" for all wireless networks must be registered with the University's NetCom department. Registration can be performed on-line at the following link: <http://www.netcom.utah.edu/poc/index.html>.
- I. Wireless access points shall require user authentication at the access point before granting access to campus or Internet services. Wireless network interfaces and end-user devices shall support authentication to access wireless networks that allow connectivity to the Campus Network Backbone.
- J. Physical security should be considered when planning the location of wireless access point and other wireless network components.
- K. Wireless passwords and data must be encrypted. No application should rely on IP address based security or reusable clear text passwords. Other methods may be allowed but require the approval of the Institutional Security Office (ISO). Information regarding wireless network encryption can be found at the following link: [http://www.it.utah.edu/services\\_it\\_admin\\_tricks\\_tips.html](http://www.it.utah.edu/services_it_admin_tricks_tips.html).
- L. Wireless networks must be designed and deployed 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, NetCom and the Institutional Security Office, under the direction of the Office of Information Technology shall resolve the interference as determined by use priority. The arbiter, in case of conflict, is the Information Technology Advisory Committee operating under the direction of ITeC.

- M. The University NetCom department and Institutional Security Office (ISO) will attempt to resolve any interference or security incidents by coordinating with the registered Point of Contact (POC) for the wireless network. If a POC is not available, the incident is resolved through administration of the network connection to the backbone.
- N. NetCom is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone. NetCom works in conjunction and cooperation with the Institutional Security Office.
- O. Disconnect Authorization

Any wireless network on campus, which poses a security threat, may be disconnected from the campus backbone network. If a serious security breach is in process, NetCom and the Institutional Security Office may disconnect the LAN immediately. Every reasonable attempt will be made to reach the registered "Point of Contact" to resolve security problems.

NetCom has the authority to disconnect any wireless network from the campus network backbone whose traffic violates practices set forth in this policy, the Office of Information Technology Network Connection Policy, or any network related policy. It is the responsibility of the college, department or division to be knowledgeable regarding the provision such policies.

- P. Grievance matters with this policy or conflicts between NetCom and/or ISO and any University college, department, or division are directed to the Office of Information Technology for resolution. The Office of Information Technology is notified within one week of the incident in question. If the conflict is not resolved to the satisfaction of NetCom or the college, department, or division, the matter may be escalated to the Information Technology/e-Commerce Executive Committee for further review and action.