Purpose

This Pace Information Technology document sets forth the policies for using wireless data technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless data radio spectrum at Pace University, NY. This policy describes how wireless technologies are to be deployed, administered and supported at Pace University. It supplements guidelines outlined in the *Pace University Appropriate Use for Information Technology Policy*, addressing issues specifically related to wireless communications including the issue of potential frequency interference.

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

- safeguard security of campus network systems
- ensure that a baseline level-of-connection service quality is provided to a diverse user community
- prevent interference with other uses of the wireless spectrum.

Scope of the Policy

The Vice President of the Information Technology/Chief Information Officer, Pace University is primarily responsible for providing a secure and reliable campus network to support the mission of the University. In order to implement this objective responsibility, the Division of Information Technology (DoIT) has promulgated campus-wide network standards (wired and wireless) to meet the networking requirements of all University constituencies and limit access to network connections which do not conform to generally accepted standard network protocols and security measures.

This policy, other relevant Pace University and DoIT IT system policies, and all applicable laws, govern the use of electronic communications resources at Pace University, NY.

Scope of Service

This policy defines the levels of service the Pace community should assume to be part of the campus wireless infrastructure. It defines the roles of DoIT and other campus units for deploying and administering the wireless infrastructure for the campus.
Network Reliability

In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). In an effort 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 wireless radio frequencies in the same way that it manages the shared use of the wired network.

While DoIT does not actively monitor use of the airspace for potential interfering devices, it responds to reports of specific devices that are suspected of causing interference and disruption of the campus network. Where interference between the campus network and other devices cannot be resolved, DoIT reserves the right to restrict the use of all wireless devices in University-owned buildings and all outdoor spaces.

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 insure 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 defines the responsibilities of DoIT and other Pace schools and departments for the planning, deployment, management and development of wireless network equipment and services. The policy describes the responsibilities of those who want wireless network facilities as well as the role of DoIT for ensuring overall integrity of the campus network.

Definitions

Access Point: An access point is a piece of wireless communications hardware, which creates a central point of wireless connectivity. Similar to a “hub”, the access point is a common connection point for devices in a wireless network. Access points can be used to connect segments of a LAN, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Similar to standard wired “hubs”, access points are shared bandwidth devices and can be connected to the wired network, allowing wireless access 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 should be specified within service level agreements.
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 wireless 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: 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 the Vice President of Information Technology/Chief Information Officer, who must approve all installations of wireless access points used on all Pace campus sites. At Pace, this approval has been delegated to the Manager, Network Operations Office, Telecommunications Department, Division of Information Technology.

- 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 Pace University.

- 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.

- Radio communication, due to its dependence on a scarce and shared resource, is subject to additional rules concerning interference and shared use.

1. Wireless access points must meet all applicable rules of regulatory agencies, such as, the Federal Communications Commission and Public Utilities Commission.
2. 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 the Vice President of Information Technology/Chief Information Officer or designee shall be used for wireless access points.
• Deployment and management of wireless access points in all areas of all campus sites is the responsibility of the Vice President of Information Technology/Chief Information Officer.

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

• Physical security of wireless access points is 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 (i.e., the wireless portion of the connection should not be relied upon by application programs to authorize use of any computer systems assets per se – the applications programs themselves must force logins and passwords etc.). In particular, no application should rely on IP address based security or reusable clear text passwords. It is expected that servers 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 shall enforce user authentication at the access point before granting access to campus or Internet services. Wireless network interfaces shall support authentication to access the campus wireless network.

**Interference:** Wireless networking equipment is an inexpensive shared medium 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 networking requires that all equipment that operate in the frequency spectrum is carefully installed and configured 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 Vice President of Information Technology/Chief Information Officer or designee shall resolve the interference as determined by use priority.

• The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list: instruction, administration, research, and public access.

**Suitability:** Wireless networks are not currently 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, faculty, and staff gather. Common areas most appropriate for wireless use include, but are not limited to, instructional labs, library facilities, public areas, and research labs.

Wireless networking is most applicable for uses such as email and web browsing. Unless using encrypted protocols, wireless devices should not normally be used for connecting to the University’s administrative systems such as human resources, payroll, student information, financial information systems, or other systems that contain confidential or sensitive information or are critical to the mission of the University.

Wireless access points provide a shared bandwidth. As the number of users increase the available bandwidth per user diminishes. Before deploying wireless networking in common areas, the advice of the Vice President of Information Technology or designee 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 networking, similar to the planning done currently for wired networking.

Users of wireless should consider all unencrypted communications over the network as insecure and available and all content as clear text.

**Responsibilities:** DoIT is responsible for:

- Creating, maintaining and updating wireless communications policy and wireless security standards. (Business Operations and Plans Department, DoIT)
- Maintaining a registration of all wireless network cards and access points on campus. (Data Network Office, Telecommunications Department, DoIT)
- Resolving wireless communication interference problems. (Data Network Office, Telecommunications Department, DoIT)
- Managing and deploying wireless communications systems in common areas of the campus. (Data Network Office, Telecommunications Department, DoIT)
- Approving wireless communication hardware and software used by University schools/departments. (Information Technology Integration Department, DoIT)
- Creating, maintaining, and updating wireless communication network security policies. (Business Operations and Plans Department, DoIT)
- Informing wireless users of security and privacy policies and procedures related to the use of wireless communications in common areas. (User Services Department, DoIT)
• Providing assistance to schools/departments for the development, management and deployment of wireless networks. (Data Network Office, Telecommunications Department, DoIT)

• Monitoring performance and security of all wireless networks within common areas and maintaining network statistics as required for preventing unauthorized access to the campus network. (Data Network Office, Telecommunications Department, DoIT)

• Monitoring the development of wireless network technologies, evaluating wireless network technology enhancements and, as appropriate, incorporating new wireless network technologies within the Pace University network infrastructure. (Data Network Office, Telecommunications Department, DoIT)

Schools, divisions and/or departments are responsible for:

• Adhering to Wireless Network Policy.

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

Authorization: Due to the lack of privacy of network communication over existing wireless network technology, all wireless traffic is presumed to be insecure and susceptible to unauthorized examination. System and/or application access authorization under wireless network technology is to be limited, as follows:

• Due to the inherent security weakness and lack of scalability of Wired Equivalency Privacy (WEP) and Server Set Identification (SSID), static WEP keys and SSIDs will not be employed as security measures. 802.1x, once the Wired Network Infrastructure is able to accommodate it, will be used, as well as MAC authentication. An inventory of University wireless cards will be distributed through DoIT’s Computer Resource Centers (computing labs). The Computer Resource Centers will also register personally-owned wireless cards using an online form.

• Wireless network users will employ encrypted protocols for transmitting sensitive and/or confidential information over a wireless network connection. These encrypted protocols include, but are not limited to, Secure Sockets Layer (SSL) for web communication, Secure Shell (Version 2), and, IPSEC.

Security Awareness: All wireless network users are to receive instructional material via a written or web publication upon registration for authentication. The instructional material will include, but not be limited to the following topics:

• Authentication for wireless network access and protection of passwords.
• Authorized use of wireless network technology.
• Wireless interference issues.
• Privacy limitations of wireless technology.
• Procedures for reporting wireless network service problems.
• Procedures for responding to a suspected privacy or security violation.
• Procedures for revoking DHCP registration due to termination of an affiliation with Pace University.

**Monitoring and Reporting:** The use of wireless network technology is to be monitored by the Data Network Office, Telecommunications Department, DoIT on a regular basis for security and performance.

1. Authentication, authorization and usage and wireless network performance reports are to be published on a monthly basis. The reports provide the following information, but are not be limited to:
   - access point availability;
   - significant security breaches or attempts

• The reports will be maintained according to Pace University’s document retention requirements.

• Any unusual wireless network event that may reflect unauthorized use of wireless network services should be immediately reported through the Data Network Office, TELED, DoIT to the Vice President of Information Technology/Chief Information Officer for review and, if appropriate, investigation. Such reportable events include the discovery of unauthorized Wireless Access Points on any Pace properties. **In all cases, the responsible University Officer is the Vice President for Information Technology/Chief Information Officer, Pace University.**

The policies stated above deal with known concerns and, in aggregate, do not necessarily form a comprehensive policy statement. Electronic communications is changing rapidly both in terms of technology and application and additional policy questions will arise in this area.

Questions concerning this or any other Information Technology Policy can be directed to doi@pace.edu.