

# Wireless Network Policy

## Purpose

- Guide the deployment and integrity of wireless networking on the Kettering University campus to ensure reliable, compatible, and secure operation
- Protect the security of Kettering University's information resources and electronic communications by specifically prohibiting access to Kettering University networks via unsecured wireless communication devices.
- Arbitrate possible interference in the FCC unlicensed 2.4 GHz and 5 GHz radio frequency spectrum
- Establish rights and responsibilities of users.

## Scope

This policy applies to all wireless network devices and uses of Wireless Local Area Network (WLAN) technologies at all physical locations on the campus of Kettering University, both inside buildings and in outdoor areas and off campus sites that connect directly to Kettering University's network backbone. Exceptions may only be granted by Kettering University's Chief Information Officer. This policy does not apply to cellular wireless technology or wireless devices and/or networks that have no direct connectivity to Kettering University's networks where those devices do not interfere with Kettering University wireless devices. This policy is subject to change as new technologies and security issues emerge.

## Authority

This policy is under the authority and oversight of the Chief Information Officer, Information Technology Department of Kettering University.

Technical review of this document is under the direction and authority of the Director of Operations, Information Technology, Kettering University.

## Technology

- Only the IEEE 802.11b and/or 802.11g standard for wireless LANs will be supported.
- All Access Points will be Cisco Aironet series or newer. **No** other vendor or model of Access Points will be permitted on the Kettering University campus. Existing non-HP or Cisco Access Points may continue to be used, but they must be replaced by the appropriate Cisco Aironet model when an upgrade or replacement is needed.
- Only the IP protocol will be supported on the Kettering University WLAN.

- The Chief Information Officer for Information Technology or designee is responsible for updates to the technology standards as the industry and technology changes.

## **Installation and Management**

- Kettering University IT Operations-Network Services (NS) will be the sole provider of design, specification, installation, operation, maintenance, and management services for all wireless Access Points. On-campus Kettering University units and affiliates wanting WLAN capability will contract with NS for installation and will be responsible for all one-time costs (e.g., hardware and software, wired network connection and power to the Access Point). Wireless equipment contracted in this manner will be owned and managed by NS. There will be no monthly or annual charges, but the requesting department may be responsible for costs associated with repair, upgrade or replacement of the devices as needed.
- Faculty, staff and students may not install or operate personal WLAN Access Points. Deviation from this policy must be presented to the CIO for consideration.
- The service demarcation point will be the Access Point itself. NS is responsible for the Access Point and the wired network to which it is attached. Departments and individual students will be responsible for all costs associated with purchase, installation, operation, and support of wireless PC cards in client computers.
- All IP addresses for the Kettering University WLAN will be assigned by a separate DHCP service maintained by NS.
- A site survey by NS must be done prior to design and installation to insure radio frequency integrity, optimum location for coverage and to facilitate connection to power and the wired data network, and to identify possible interference problems.
- Installation must comply with all health, safety, building, and fire codes.
- In cases where the device is being used for a specific teaching or research application, NS will work with faculty to mitigate any security issues and accommodate the device without disrupting the Kettering University WLAN.

## **Radio Signal Interference**

- 802.11b/g WLANs operate in the unlicensed 2.4 GHz range and conform to the IEEE 802.11 DSSS (Direct Sequence Spread Spectrum) specification. Other wireless devices use the same 2.4 GHz frequency band and may disrupt the operation of the Kettering University wireless network. These include cordless phones, cameras, keyboards, mice, audio speakers, and other wireless LAN devices (like Bluetooth and earlier versions of 802.11). To assure the highest level of service to WLAN clients, the use of all other 2.4 and 5 GHz devices should be discontinued on the Kettering University campus.
- The Chief Information Officer for Information Technology or designee has the authority to require the cessation of unauthorized use of the 2.4 and 5 GHz bands.

## Security/Access

- All campus WLANs will use SSL for authentication for security, with exceptions for special circumstances approved by NS.
- All Access Points and wireless client adapters on the Kettering University WLAN will use an SSID maintained by NS.
- A valid Kettering University Computing ID is required to use the Kettering University WLAN & LAN.
- Given the relatively weak security of WLANs, people are encouraged to use applications that support encryption such as SSL-based secure websites and Secure Shell (SSH) instead of Telnet.

## Restrictions

- Broadcast frequencies used by the wireless network will be monitored on Kettering University property. Devices that interfere with the wireless network may be subject to restriction or removal.
- Use of the wireless network is subject to the general restrictions of Kettering University's Computer and Network Acceptable Use Policy.
- Only authenticated access to the Kettering University's wireless network is permitted. Logs may be used for assessing network problems or identifying unauthorized or unacceptable use of the wireless network.

## Limited Support

- The wireless network's maximum data speed is less than 1/10<sup>th</sup> the speed of the campus wired network. High bandwidth applications like large file transfers, Microsoft Windows system updates, and media sharing or peer to peer with programs are not supported.
- Performance varies and cannot be guaranteed.
- Off-campus connections to the wireless network are not supported.

## Background

The Kettering University wireless network is designed to be a convenient supplement to the wired network for general functions including web browsing, email and printing to public printers. Wireless "access points" located in many areas of campus, allow suitably configured computers equipped with wireless network cards to make wireless connections to the campus network.

Despite these advantages, 802.11b/g WLANs have their limitations. For example, they are an order of magnitude slower than wired LANs. Despite claims of 11 Megabits per second (Mbps) of bandwidth, the practical limit is about 5 Mbps - and that's shared among all people using that Access Point. Wireless radio signals are shared by everyone connected to the same wireless access point. As the number of wireless connections increases, the bandwidth available to each connection decreases and performance deteriorates. Distance from the access point, buildings or objects shielding the access

point, signal interference, quality of your equipment, battery power and other factors may also impact performance. Consequently, it is not hard for one person to monopolize the bandwidth of an Access Point and kill the performance for the other people using it. Applications that generate high network traffic do not work well on wireless networks and negatively impact performance for everyone connected to the same access point. Compare that to a typical wired, switched network connection on the Kettering University campus that is dedicated to one computer and operates at 100 Mbps in full duplex (i.e., you get nearly the full 100 Mbps in both directions - incoming and outgoing data traffic). WLANs are also inherently insecure. Tools are readily available to capture data packets from the airwaves and thereby "snoop" on someone else's communications. Consequently, wireless users must take extra precautions and adhere to standards to ensure secure communications over a WLAN.

While the standard does allow a wireless PC card from one vendor to connect to an Access Point from another vendor, the devices must all be carefully configured to support this and every product has proprietary features that don't always interoperate with other wireless products. This is especially true when it comes to security and management. Consequently, a Kettering University WLAN security standard and central management of the campus "air space" are necessary to protect valuable information resources and to ensure the highest degree of interoperability as one moves from one location to another on campus with a wireless-equipped computer.

To promote efficient and secure wireless network access, Kettering University maintains strict standards for the deployment of wireless devices.

## **Definitions**

*802.11b:* An IEEE standard for wireless data networking rated at 11 Megabits per second throughput operating in the FCC unlicensed 2.4 GHz Industrial/Scientific/Medical (ISM) band and using Direct Sequence Spread Spectrum (DSSS) technology to transmit the signal. The range of the signal indoors is up to 150 feet at 11 Mbps (300 feet diameter), or 800 feet outdoors. The range and strength of the signal are reduced significantly as it passes through walls, floors, and other physical structures.

*Access Point:* A hardware device that serves as a communications "hub" for wireless clients and provides a connection to the wired LAN.

*Kettering University Computing ID:* The computer account allocated to an individual that provides access to centrally managed information technology (IT) resources such as e-mail, Web, Unix, and file space. The Kettering University Computing ID has the following attributes: a user ID (a.k.a. the "login name"), a password, an e-mail address (*userID@kettering.edu*, disk space for storing files, Web and Internet access, and a personal web page if desired (<http://www.kettering.edu/~userID>). See <http://www.kettering.edu/computingID> for more information.

*SSID:* The "Service Set Identifier" may be used as a relatively insecure security key for a WLAN, somewhat like a password. If the SSID is set in the Access Point, then only client wireless cards configured with the same SSID may connect to that Access Point.

*WEP* "Wired Equivalent Privacy" that provides limited security to a wireless connection by encrypting all data transmitted between the computer and the Access Point. At this time, 40-bit and 128-bit WEP is available on most vendors' Access Points and Kettering University supports both.

*Wireless PC Card:* Hardware device in a client computer (most often a card that fits in a PCMCIA Type II slot in a notebook computer) that communicates with an Access Point via radio signals (i.e., without wires). Also known as "wireless client adapter".

*WLAN:* "Wireless Local Area Network". The term often used for a wireless network within a limited area consisting of one or more wireless Access Points that provide network connectivity to computers equipped with wireless capability (usually a notebook computer with a wireless PC card). In essence, a WLAN provides the functionality of a wired LAN without the physical constraints of the wire.

This document used the wireless policy developed by the Kansas State University as a template.

Reviewed: 11/8/07 dek