PELLISSIPPI STATE COMMUNITY COLLEGE

POLICY 08:13:09
WIRELESS NETWORK POLICY

I. Purpose

This document contains the provisions for using wireless technologies and assigns responsibilities for the deployment of wireless services and for the administration of the wireless radio frequency spectrum in a distributed campus network environment. This policy expands Pellissippi State Policy 08:13:05 - Computer System Use, by including specific direction regarding wireless communications.

II. Scope

Pellissippi State Community College is responsible for providing a secure and reliable campus network. Network and Technical Services (NTS) shall be responsible for providing services within the scope of this policy. This will be accomplished by the use of campus-wide network standards and policies and by limiting access to data network connections that are not in compliance.

This policy applies to all wireless network devices utilizing the College's Internet Protocol (IP) space (including private IP space within the College networks) and all users of such devices. It 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, including satellite locations.

III. Definitions

A. Wireless Network - local area network technology that uses radio frequency spectrum to connect computing devices to a wired port on the campus network to enable connection to the campus network backbone and the Internet.

B. Access Point - electronic hardware that serves as a common connection point for devices in a wireless network LAN group. An access point acts as a network hub that is used to connect segments of a LAN, using transmit and receive antennas instead of wired 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 - wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

D. Interference - 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.

E. Privacy - the condition that provides for the confidentiality of student, faculty and staff communications, and institutional data transmitted over a wireless network.

F. Client hardware/software - the electronic equipment and software that are installed in a desktop, laptop, handheld, portable, or other computing device to provide a LAN interface to a wireless network.

G. Rogue Access Points - access points that are not managed and controlled by the NTS group.

IV. Provisions

A. All acceptable use provisions of Pellissippi State Policy 08:13:05 - Computer System Use 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.

B. Deployment and management of wireless access points will be maintained by the NTS Department. Unauthorized access points or "Rogue Access Points" are prohibited from being attached to Pellissippi State's network.

C. Wireless access points shall require user authentication at the access point by means of an Active Directory Account before granting access to any campus services. Wireless network interfaces and end-user devices shall support authentication to access wireless networks that allow connectivity to the campus network backbone. Guest access to the Internet without authentication is supported by agreement with the acceptable use policy. The wireless network will be treated as an untrusted network. Password and data protection is the responsibility of the application. The wireless infrastructure will not provide specialized encryption 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 and/or require their own general or applications authentication, authorization and encryption mechanisms to be used by clients entering from any unprotected network.

D. 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 College. Telnet will not be permitted as it transmits in clear text.

E. NTS 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.

F. 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, the NTS Group may disconnect the WLAN immediately. The Network group has the authority to disconnect any wireless network from the campus network backbone whose traffic violates practices set forth in this policy, Pellissippi State Policy 08:13:05 - Computer System Use, or any network related policy.

V. 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.

Approved: President Allen G. Edwards, June 16, 2003
Reviewed/Recommended: President's Staff, March 2, 2009
Approved: President Allen G. Edwards, March 2, 2009
Editorial Changes: July 1, 2009
Reviewed/Recommended: President's Council, May 19, 2014
Approved: President L. Anthony Wise, Jr., May 19, 2014