POLICY 08:13:09
Wireless Network
Administration and Access

I. Purpose

The purpose of this policy is to define provisions for protecting and using the College's wireless infrastructure and to assign responsibilities for the deployment and administration of wireless services and the wireless radio frequency spectrum in a distributed campus network environment. This policy expands Pellissippi State Policy 08:13:01 Information Technology Acceptable Use, by including specific direction regarding wireless communications.

II. Scope and Applicability

This policy 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 all administrative, academic, and other areas which are part of the College's campuses including any outdoor spaces on the campus. This policy also 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.

This includes but is not limited to:

- Faculty, including adjunct faculty and temporary full-time faculty
- Staff, including full-time, temporary part-time and other contracted employees
- Students
- Third party vendors that have been granted access to any college wireless network
- Guests of the college who have been granted access to any college wireless network
- All other parties with access to the college wireless network

III. Risks, Liabilities and Disclaimers

The College makes available wireless networks computing systems and resources consisting of hardware, software accounts and communication technologies for wireless access to campus resources and the internet. 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. The College accepts no responsibility for any loss of data or damage to data or services arising directly or indirectly from the use of these systems and resources or for any consequential loss or damage. The College makes no warranty, express or implied, regarding the services offered or their fitness for any particular purpose.

Use of these wireless networks and resources signify the following:

- The user agrees to comply with the provisions of this Wireless Network Access Policy.
- The user accepts responsibility for knowing the contents of this policy statement. Failure to read or acknowledge this statement will not be an excuse for noncompliance.

- The user accepts that failure to comply with this policy may result in temporary or permanent denial of access to computer or information technologies, or in some cases may result in college disciplinary action or legal action.

IV. Definitions

Access Point - electronic hardware that serves as a common connection point for devices in a wireless local area network or LAN. 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. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the campus network backbone.

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.

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.

Rogue Access Points - access points that are not managed and controlled by the staff within Information Services.

Wireless Infrastructure - wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Wireless Local Area Network or WLAN - 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.

V. Policy and User Responsibilities

A. Policy

Pellissippi State Community College is responsible for providing a secure and reliable campus network to ensure the confidentiality, integrity, and availability of technology and data. This is accomplished through the development and implementation of compliance standards which address security requirements and expectations for acceptable use of computer systems, including the wireless network and by limiting access to data network connections that are not in compliance. Network and Technical Services (NTS) shall be responsible for providing services within the scope of this policy.

The College has adopted approved standard protocols for wireless networking of the Institute of Electrical and Electronic Engineers, Inc. (IEEE) and will deploy access points with these protocols to ensure that adjacent access points with slightly overlapping areas of coverage do not interfere with each other. NTS staff will manage the shared use of unlicensed frequencies for the campus community and campus authority to resolve any interference issues.

Deployment and management of wireless access points will be maintained by staff in information Services. Unauthorized access points or "Rogue Access Points" are prohibited from being attached to Pellissippi State's network.

The appropriate Information Services employees are 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, availability and security of the campus network backbone. Priority for wireless activity will be given to use of College-owned or –provided resources.

B. User Responsibilities

As a user of Pellissippi State Community College's technology resources, you have a shared responsibility with the College Information Services staff to maintain the integrity, confidentiality and availability of our systems, services, and data. Your responsibilities include:

All users of the wireless network must follow Pellissippi State Policy 08:13:01 Information Technology Acceptable Use. Any user who connects a personally owned computer or other device must follow Pellissippi State Policy No. 08:13:06 Bring Your Own Device (BYOD).

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.

Wireless access points shall require user authentication at the access point by means of an Active Directory Account or a guest account as defined in Policy 08:13:02 Computer 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 guest wireless network (PSCC_GUEST) will be treated as an untrusted network and it will be the user's responsibility to protect their personal device.

Faculty, students, staff and guests are individually responsible for the proper use of their accounts, including proper password creation and protection and appropriate use of Internet resources. 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.

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. Programs requiring remote connections must utilize SSH as communication standard.

VI. Enforcement

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.

Possible violations of this policy, other campus policies or illegal activity may have other disciplinary actions taken as listed in Pellissippi State Policy 08:13:05 Computer System

Use. Disciplinary actions will conform with other college policies and may result in a disciplinary review conducted by the vice president of Student Affairs, or designee, in matters involving alleged violations by students, or by the director of Human Resources in matters involving employees of the College.

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
Reviewed/Recommended: President's Council, September 9, 2019
Approved: President L. Anthony Wise Jr., September 9, 2019