Wireless Local Area Network (LAN) Management

OVERVIEW

Wireless networks allow for accelerated delivery of network connectivity at a lower cost than traditional wired networks. Because of this, wireless networks have overtaken wired networks in terms of total data transmitted and have become a cornerstone of digital service delivery. Wireless networks present unique challenges in their administration, including the following:

- **Shared Spectrum** – Wireless data networks using the IEEE 802.11 specification operate in the 2.4 GHz or 5 GHz radio spectrums. Both frequencies must be shared by all applications utilizing them in the same coverage area. This can be a problem if adjacent departments in the same building or area independently operate wireless local area networks (LANs). Problems may also be caused in the 2.4 GHz spectrum by other competing applications, such as microwave ovens or some cordless telephones.

- **Nonoverlapping Channels** – Both frequencies are limited by the number of nonoverlapping channels that are available with the 2.4 GHz frequency limited to only three nonoverlapping channels and the 5 GHz frequency limited to 23 nonoverlapping channels.

- **Security** – Wireless networks have unique security requirements to prevent rogue devices from connecting to, or interfering with, the WSU network.

For the above reasons the following requirements are necessary.

See *BPPM* 87.01 for definitions related to this section.

Purpose

The wireless LAN policy (*BPPM* 87.35) provides assurance of the security and operability of the wireless LAN segments thought out the University.

Scope

This policy applies to all institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit institutional data.

POLICY

Information owners are accountable for developing appropriate procedures for the implementation of this policy.

IMPORTANT: Information owners are to develop procedures to implement this policy (*BPPM* 87.35) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

New 7-20
Information Technology Services
509-335-4357

Wireless Local Area Network (LAN) Management

Management

To ensure the technical coordination required to provide the best possible wireless network for Washington State University, central information technology departments are solely responsible for the deployment and management of 802.11 access points or other related wireless technologies. The central information technology departments are WSU Information Technology Services (ITS) in Pullman, and ITS in Spokane, Tri-Cities, Vancouver, and Everett, hereafter referred to collectively as central ITS.

Departments should not deploy 802.11 access points or other related wireless technologies without coordination with the appropriate central ITS group.

Deployment

Wireless access is to be deployed in a manner such that access meets the greater needs of the campus and usage is not to be restricted to a specific use and/or department.

Equipment

In order to maintain compatibility between the various components of the wireless LAN and to provide spare equipment in case of failure, central ITS specifies the equipment to be used in the wireless LAN.

Security

Shared Spectrum Management

Due to the shared nature of the wireless spectrum and the need for security and reliable service delivery, unauthorized equipment that interferes with approved equipment or that does not comply with the security requirement needs to be modified or replaced.

The appropriate ITS group works with the owner of the equipment to resolve problems; however if no solution is found, the equipment is disconnected.

Departments planning new installations are to ensure that they work with the appropriate ITS group to avoid these issues.

Rogue Devices

To prevent unauthorized clients, all wireless access is to be connected to ITS-managed authentication services. Unauthenticated access to services on the WSU wireless LAN is not permitted. Authentication services include, but may not be limited to, MAC Auth and 802.1X Auth.

ITS monitors for rogue access points which are connected to the WSU wired network, but are not authorized to deliver wireless networking. When detected, ITS shuts the wired network ports of rogue access points.

Wireless Local Area Network (LAN) Management

Rogue Devices (cont.)

ITS monitors for imposter access points, which are not connected to the WSU wired network but advertise an official WSU SSID (service set identifier). When detected, ITS investigates imposter access points.

IoT and Bluetooth

IoT devices must be connected to the WSU Guest network, or to a dedicated SSID that ITS provisions for IOT devices.

Bluetooth network connectivity is not supported on the WSU wireless network.

Definitions

IoT

Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Bluetooth

Bluetooth is an open wireless technology standard for transmitting fixed and mobile electronic device data over short distances using short-wavelength radio waves in the 2.402 GHz to 2.480 GHz range. It is used primarily to establish wireless personal area networks (WPANs), allowing users to form ad hoc networks between a wide variety of devices to transfer voice and data.

ENFORCEMENT

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University or state policies and handbooks (e.g., the WSU *Faculty Manual*, the *Administrative Professional Handbook*, *WAC* 357-40 (civil service employees), applicable collective bargaining agreements, or the WSU Standards of Conduct for Students, *WAC* 504-26).

Exceptions

Exceptions to this policy are managed and maintained by the Office of the CIO, under the guidance of the University Chief Information Security Officer (CSIO).

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

Wireless Local Area Network (LAN) Management

MAINTENANCE

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, standards, or regulatory requirements.