Marshall University Information Technology Council

Procedure ITP-18

Marshall University Wireless Communications and Networking Procedure

1. General Information

1.1. Scope:

This procedure applies to all wireless transmission in any of the unlicensed frequency space including radio, infrared, and free space optical at any Marshall University owned, rented, or leased properties. It also applies to FCC licensed communications activities that originate from any university owned, rented, or leased space including cellular telephone towers or micro cells, radio broadcast stations, two- way radios, television broadcasts, analog/digital microwave & satellite, or any other wireless communications and networking technology.

1.2. Passage Date:

November 6, 2015

1.3. Effective Date:

January 26, 2004.

1.4. Revision Date:

August 19, 2019

1.5. Purpose:

The purpose of this procedure is to ensure reliable, secure, and cost effective wireless communications and networking services at Marshall University. Wireless communications and networking use the shared resource of electro-magnetic frequencies in the shared air space of campus facilities and property. Given the innate security issues with wireless communication and the possibility of one device interfering with another; careful planning is required to support the implementation of secure, reliable, and cost effective wireless communications services across the Marshall University campuses and at remote facility locations.

This procedure serves to clarify for Wireless Local Area Network (WLAN) technologies existing applicable policies and procedures including ITP-16 IT Infrastructure Authorization Procedure (1996/rev. 2015), ITP-15 Intra-Campus Wiring Procedure (1996/rev. 2010), and ITP-17 the Information Technology Cost Recovery Procedure (1991/rev. 2015). It also serves to designate responsibility and governance of the use of unlicensed FCC frequencies and the coordination of FCC licensed frequencies on Marshall University owned, rented, and leased properties.

A wireless communications & networking procedure is essential:

1.5.1. To limit interference with the University's communications & network infrastructure

1.5.2. To promote greater security in campus communications & networking devices

1.5.3. To provide a consistent interface and procedures for use by the Marshall community

1.5.4. To identify responsibility and management entities

1.5.5. To identify acquisition & installation procedures

2. Procedure

2.1. Ownership responsibility and management of radio airspace.

2.1.1. Marshall University is the owner of the unlicensed radio frequencies on campus. These include the FCC 2.4 GHz Industrial/Scientific/Medical (ISM) and the 5 GHz Unlicensed National Information Infrastructure (UNII) bands used in WLAN. Information Technology (IT) is responsible for managing these radio frequencies for the benefit of the entire University community. IT may restrict use of any device(s) that in its opinion can cause interference and/or impact the university use of the unlicensed radio frequencies ranges. This includes WLAN access points, consumer oriented wireless devices such as wireless/cordless telephones, and radio frequency remote controls as well as other transmission and/or receiving devices.

2.1.2. IT is solely responsible for providing WLAN services on any university property, including intra-building, inter-building, and connectivity to commercial service providers. No other department or entity may deploy WLAN access points or other wireless services on campus. Private wireless access points in the residence halls, offices, classrooms, and public areas are strictly prohibited.

2.1.3. WLAN technologies will be offered on a cost recovery and life-cycle maintenance charge back basis to non-core university units just as MUNet wired LAN service has been since the early 1980's and will be itemized as part of the annual IT Services Rate schedule.

2.1.4. IT is responsible for maintaining a secure WLAN network and will deploy adequate security measures and procedures to support WLANs at all university campuses and in University sponsored facilities.

2.1.5. IT will deploy a campus wireless network as University units request service based on available funding.

2.1.6. IT will work with departments to attempt to accommodate special needs, where technically feasible and cost justifiable.

2.1.7. IT will collaborate with academic departments where devices used for specific educational or research applications may require specific solutions.

2.1.8. IT will develop a procedure for the temporary use of WLAN access points to support campus events on a cost recovery basis.

2.1.9. Unit's sponsoring WLAN services will supply this service to any MUNet account holder that is in the service range of the IT installed access point.

2.1.10. IT will review all requests submitted in writing for the deployment of FCC regulated transmission services to or from campus facilities and provide an analysis of the impact to the Office of the Senior Vice President for Information Technology/CIO within thirty (30) days of the request.

2.1.11. Owners of mobile devices agree to abide by all security policies and MUNet device standards.

2.2. WLAN Installation Procedure

2.2.1. University Units desiring WLAN coverage in their area shall contact the IT Service Desk and log a call requesting that a WLAN site survey be conducted by the IT Infrastructure group based on available funding.

2.2.2. IT Infrastructure will conduct a WLAN site survey and provide a report to the unit that consists of possible coverage areas, anticipated signal strength, environmental noise concerns, cost projections and estimated service installation time after receipt of an order for the services.

2.2.3. Upon receipt of a purchase agreement from the non-core unit for WLAN services, IT will purchase and install the equipment and services necessary to provide the service.

2.2.4. IT will provide instructions to the user for installation, wireless access cards, and/or other security software or procedures necessary at the time of installation.

2.2.5. IT will provide regular firmware and software updates upon receipt of written notification from the hardware vendor of update availability and after said update has been tested by IT Infrastructure staff on non-production equipment.

2.3. WLAN Service Considerations

2.3.1. Wireless networking has bandwidth limitations compared to the wired networks. The bandwidth is shared among other users and should not be considered a replacement for wired service. The wireless network should be viewed as augmenting the wired network, to provide more flexible network use of primarily portable devices. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for WLANs.

2.3.2. Mobile devices that are carried off-campus and used on non-university WLANs that may not be secured should take special precautions in using VPN and personal firewall software and/or other technologies to eliminate security risks. These other WLAN locations may be telecommuter homes, airports, hotels, or public hot spots providing 802.11 services. Users are encouraged to consult with an IT security specialist if they plan to use devices off-campus.

2.4. WLAN Standards supported

2.4.1. 802.11g – IEEE 802.11g provides a maximum 54 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency. 802.11a – IEEE 802.11a provides 54 Mbps of shared bandwidth per access point using the 5 GHz radio frequency. 802.11n – IEEE 802.11n operates on the 2.4 GHz radio frequency and the 5 GHz radio frequency with a maximum of 600 Mbps using the 5 GHz radio frequency. 802.11ac – IEEE 802.11ac allows for theoretical speeds up to 6.9 Gbps using the 5 GHz frequency. IT provides 802.11g, 802.11a, 802.11n and 802.11ac wireless services.

2.4.2. 802.1x using EAP-TLS and/or PEAP will be used for client authentication. Additional security procedures may be applied as needed.

2.4.3. Security for WLAN transmission follows the WPA2 802.11i standard. This standard is intended to improve WLAN security. It describes the encrypted transmission of data between systems of 802.11 WLANs. It defines encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES).

2.5. FCC Licensed Wireless Review Process

2.5.1. All FCC forms must be completed and submitted to IT Infrastructure prior to their submission for FCC approval. All path studies must be included.

2.5.2. IT Infrastructure must be allowed thirty (30) business days for the review of all such requests.

2.5.3. Impact on the university will be assessed and a final decision for approval will be reviewed by the Office of the Senior Vice President for Information Technology/CIO in consultation with the Office of the President.

2.5.4. If approved, final submission to the FCC will be completed.

2.6. Enforcement

The Office of the Chief Information Officer is the procedure administrator. This office delegates the enforcement of the procedure to the Director of IT Infrastructure. Devices and services violating this procedure will be confiscated and service terminated pending review.