PERSONAL WIRELESS HOTSPOTS

GENERAL

Some portions of the Texas A&M University Commerce campus do not have facilities for wireless network access. In the residence halls, residents are allowed to setup wireless access points that do not cause interference.

APPLICABILITY

This standard administrative procedure applies only in the residence halls where wireless network access is not provided by A&M-Commerce. This procedure does not apply in administrative or classroom buildings.

PROCEDURES

1. Students must confirm with Residence Life and Technology Services that wireless network access is not currently offered in their residence hall.

WIRELESS NETWORK NAMING

1. The wireless network SSID should be set as "Building Name" and "Room Number". For example "Jones Hall 222."
2. The wireless network SSID should not begin with TAMUC. A&M Commerce uses this prefix on all of its official wireless networks, currently including TAMUC and TAMUCHOUSING, but this usage may be expanded in the future.
3. The wireless network may be configured to either broadcast or hide its network SSID.

ACCOUNTING AND RESPONSIBILITY

1. Students are responsible for their own wireless network security policy. All devices connected to the same wireless access point will appear to be in the room where the wireless access point is located.
2. The resident(s) of the room are responsible for all network activity originating from their assigned room.

SECURING WIRELESS ACCESS

1. The wireless access point should be configured to require a password and use encryption. This is automatic with most current equipment.
2. WPA2 is the preferred wireless encryption standard. WEP encryption is insufficient and should not be used.

NON-INTERFERENCE

1. If the university includes a residence hall in the campus wireless network, no personal wireless hotspots may be added in that residence hall, and existing wireless hotspots must be removed.

2. IEEE 802.11b and 802.11g standards allow for only 3 usable channels. IEEE 802.11a and 802.11n allow for more usable channels. It is recommended to pick a channel with a minimum level of interference.
3. If a personal wireless hotspot causes interference with another user's hotspot, or with the university network, it may be disabled, or in severe cases, removed at the University's discretion.
4. The resident(s) of the room where the equipment is found will be notified of the interference and offered a chance to correct it

REMOVAL OF EQUIPMENT

1. If personal hotspot equipment is left behind after move-out, it will be considered abandoned and disposed of according to existing university procedures.
2. If personal hotspot equipment is removed by Information Technology, it will be held by Information Technology for 30 days. If equipment is not claimed within 30 days, it will be sent to the University Police department for disposal according to existing university procedures.

RELATED STATUTES, POLICIES, AND REQUIREMENTS

Information Security Standard Administrative Procedure for Wireless Access
University Rule 21.99.04.R1 Disposition of Abandoned and Unclaimed Personal Property

HISTORY

First Publication – September 20, 2013