OIS 38 – Standard for Wireless Network

I. STANDARD STATEMENT

This standard applies to the deployment and operation of all university owned or operated wireless devices and all other devices connected to university infrastructure services on the UTSA campus.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. UTSA campuses have three separate wireless (or Wi-Fi) networks.
B. Because UTSA must ensure that the faculty/staff and student wireless networks are used only by faculty, staff, and students, the university requires authentication. Therefore, to use the AirRowdy Fac/Staff or Student networks, it will be necessary for users to provide a UTSA network username and password.
C. The wireless guest network is available for visitors and guests that provide a valid email address. Only the AirRowdy Fac/Staff network is encrypted and secured against network eavesdropping. All users of UTSA's wireless networks are subject to the UTSA Acceptable Use Policy.
    1. All wireless access points are considered an extension of UTSA's infrastructure, and are owned, maintained, and supported by UTS. Technical staff members are available to deploy wireless coverage in on-campus offices, meeting rooms, laboratories, or departmental space.
    2. The use of unapproved wireless access points is prohibited. Improperly configured devices can cause serious harm to both the wired and wireless network, and negatively impact network services for other clients.

3. Confidential and/or sensitive UTSA data must not be transmitted via wireless methods to or from a portable computing device unless approved wireless transmission protocols, along with approved encryption techniques, are utilized. Therefore, confidential and/or sensitive UTSA data must not be sent across the guest or student networks, as these networks are unencrypted, and information is sent "in the clear" and subject to interception.
4. Wireless network access deployment and operation must be consistent with the university's mission, strategies, directions, and initiatives.

Title: OIS 38 – Standard for Wireless Network
Effective Date: August 31, 2011
Last Reviewed: August 13, 2020