THE UNIVERSITY OF ARIZONA.
Arizona's First University.

Standard Title: Wireless Deployment and Maintenance
Standard Number: IS-S601
Responsible Office: Information Security Office

Wireless in the Local Area *Network* using the IEEE 802.11 standard is a fast emerging technology. 802.11 wireless technologies are by nature easy to deploy, but highly sensitive to RF interference. Because of these characteristics, all wireless use must be planned, deployed, and managed in a very careful and centralized fashion to ensure basic functionality, maximum bandwidth, and a secure *network.*

The use of wireless *network* technology must not reduce the *availability*, *integrity* and *confidentiality* of *university resources*. Accordingly, any implementation of wireless *network* systems at the university should meet or exceed the following standards.

To ensure the technical coordination required to provide the best possible wireless *network* for the university, Network Technology Solutions (NTS) will be responsible for the oversight of all 802.11 and related wireless technology on the campus. No other entity may deploy 802.11 or related wireless technology that attaches to the *university network* without coordination with NTS.

These following minimum standards provide the structure for a campus-wide solution. The implementation of wireless technology includes centralized *authentication* and *authorization*.

The standard addresses the following:

- The deployment of 802.11 and related wireless technology.
- The provision of wireless service for campus *units*.
- The management of 802.11 and related wireless technology.

1. Access Points

NTS has the authority to minimize interference to the common wireless *network*, and will work with *units* to reconfigure or shut down any wireless *network* implemented by a *unit* that interferes with the university wireless *network* as a whole.

The following applies to all university Wireless Access Points:

- All university wireless must use an enterprise level access point compatible with 802.1x and variations of EAP.
- External antennas must comply with all federal and state regulations for antennas.
- Equipment mounted on external structures must be approved prior to installation.

- Installation of access points and bridging *devices* must be consistent with health, building, and fire codes.

2. Authentication

All university wireless must activate IEEE 802.1X to authenticate and control user traffic to a protected *network* and use a variation of EAP to encrypt username/password combination.

3. Security

All university wireless *networks* must use WPA/WPA2 to access *network* resources unless an exception has been granted by the *UISO*.

4. Monitoring & Reporting

The use of wireless *network* technology is to be monitored on a regular basis for security and performance.

All wireless *network* service problems should be reported to NTS.

Any unusual wireless *network* event that may reflect unauthorized use of wireless *network* services will be immediately reported by the wireless system administrator to *NTS SecOps* for review and, if appropriate, investigation.

5. Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline.

Revision History

Initial Draft	08/09/07
Effective Date	05/27/08