Management of UTnet Wireless Access Policy

1. Requirements

Responsible management of wireless access to the campus network infrastructure, UTnet, requires adoption of the following policies throughout The University of Texas at Austin:

All wireless access to university networks shall be designed, installed, and operated by Information Technology Services-Networking. Individuals and departments are prohibited from extending university networks through means of wireless technologies.

All wireless access to university networks shall be authenticated by ITS-approved methods. Students, faculty, staff and official visitors at the university must access the campus wireless network using the encrypted network, 'utexas'.

Guests may utilize the 'attwifi' unencrypted network (account holder, credit card, or coupon).

The primary goal of all wireless designs shall be ubiquitous service to the broad university community. Private interests are secondary design criteria. Wireless networks shall be independent of local wired networks.

Wireless services should be considered "best effort" and not suited for activities requiring highly reliable service levels.

Limited exceptions to these policies may be granted in writing by ITS Networking (e.g., a wireless research group's experimenting with isolated wireless devices). Submit requests for exceptions by e-mail to networking@its.utexas.edu.

2. Rationale

UTnet is a ubiquitous communication infrastructure at the university, connecting in excess of 300,000 devices across the campus. The technology that implements UTnet and the applications it supports has evolved rapidly over nearly two decades. Beginning as an experimental network for a small set of researchers, UTnet now carries all of the university's Internet-based traffic. Some of the traffic, including all university Web traffic, electronic mail, and transactions with the administrative computing system, supports activities that are familiar to many campus users. Other types of traffic support less common, but no less critical, institutional applications, including facilities control and monitoring systems (FCMS), building-access control systems, cafeteria authorization and accounting, and surveillance monitors. Even production voice telephony is carried by the network. UTnet wireless service, with over 8,000 access points, is an important component of the university's communications infrastructure.

The UT community expects UTnet to be operated at a high level of reliability and availability. Given the essential applications supported, network services are required continuously. When a network failure occurs, return-to-service time must be minimized. This requires extensive controls, monitoring, and coordination of the system as whole.

Wireless networks pose significant challenges to stable and reliable operations of the campus network. The very flexibility and dynamism of wireless can inadvertently circumvent network topologies and security profiles in unpredictable ways, leading to failures and security exposure of critical infrastructure. Centrally designed and controlled wireless networks help to mitigate these exposures and reduce the time to troubleshoot problems when they occur.

Authentication for wireless networks is particularly important to enable notification of the owner of an improperly configured or malfunctioning device that interferes with normal network operations. Authentication also deters rogue activity and enables the university to assist law enforcement agencies as they investigate possible criminal activity. Absent authentication of wireless sessions, the networks in all buildings supporting unauthenticated connections are susceptible to failures unique to the local implementations, which could potentially affect critical infrastructure campus-wide.

Wireless networking, as implied by its name, has no dedicated medium–unlike wired systems. Signals used to convey data radiate across an uncontrolled spectrum at low power levels, competing with all other radiating sources (other computers, other wireless technologies, elevators, machinery, etc.). Isolating and troubleshooting problems or guaranteeing resources in such a dynamic environment is extremely difficult, and in some cases beyond current technical abilities. Necessarily, support for wireless systems is "best effort." In contrast, wired systems provide a dedicated medium, the wire, and dedicated network equipment for the individual computers being connected, each of which can be easily isolated for troubleshooting, repair, and performance enhancements in a minimum amount of time. Consequently, activities requiring robust service levels should be supported on wired networks.

3. Revision History

Version	Date	New	Original
	5/29/2018	1. Updated guest acccess requirement 2. Updated number of devices connected across campus by UTnet to 300,000 3. Updated number of access points to 8,000	1. "Sponsored guests may use the unencrypted open network 'guest.utexas.edu'" 2. "60,000" 3. " 2,500 IEEE 802.11"
Management of UTnet Wireless Access	10/03/2013	Converted PDF to web page.	
Management of UTnet Wireless Access	3/9/2011	• Converted web page to PDF. • Added Requirements as the first section heading.	
	10/1/2009	• Updated visual appearance to new template. • Corrected any out of date links to ensure they are pointing to the most current policy documents.	
	07/01/2008	1. Corrected the SSID name for non-affiliated guests to 'guest.utexas.edu.' 2. Changed the type of guest using the network to "Sponsored." 3. Corrected the number of access points to "2,500."	1. "utexas" 2. "Non-affiliated" 3. "2,200"
	3/29/2007	Corrected the SSID name for non-affiliated guests to "utexas."	
	3/28/2007	1. Change log created 2. Updated to replace Public Network Authentication system reference 3. New text: "Students, faculty, staff and official visitors at the university must access the campus wireless network using the encrypted network, 'utexas' Non-affiliated guests may use the unencrypted open network 'guest.utexas.edu.'" 4. Updated count of 802.11 access points to 2,200	4. "1,400"

4. Approvals

Name	Role	Date
Information Technology Services- Networking	Approval	7/1/2008