

Wireless Policy

This Wireless Usage Policy applies to all workstations, notebooks, wireless local area networks, systems, servers and software applications used on campus. It also applies to all staff, faculty, and students at UST. The purpose of this policy is to ensure the security, reliability and utilization of the wireless network.

Wireless Network and Internet access is available on the University of St Thomas campus. Due to the nature of wireless communication, wireless networking requires increased cooperation between faculty, staff and students in order to fully maximize the benefits of this technology.

After connecting to the wireless network, the University community may use it to access the internet. Access to network resources such as share drives, printers, etc. will not be permitted without prior coordination with IT.

Institutional Purposes

The purpose of this policy is to inform users of the acceptable use regulations related to UST's wireless network. This policy has been put in place to protect the staff, faculty, and students and to prevent inappropriate use of wireless network access that may expose UST to multiple risks including viruses, network attacks and various administrative and legal issues.

This policy has been created to expand on the Acceptable Use Policy by including specific information regarding the use of wireless networking and data access on campus.

This policy is subject to change as new technologies and methods of implementing these technologies emerge.

General Use

It is the intention of IT to provide a high level of reliability and privacy when using the wireless network. Wireless access points are distributed around the campus in order to provide and maintain availability. Wireless access points provide a shared bandwidth and so as the number of users increase the available bandwidth per user decreases. As such users are asked to be considerate of other users and refrain from running high bandwidth applications and operations such as downloading large music files and video from the internet.

Network reliability is determined by the level of user traffic and accessibility. In order to provide an acceptable level of reliability bandwidth will be regulated according to user role and location. UST cannot guarantee the confidentiality of any information stored on any device connected to the UST Wireless Network; therefore the wireless network should not be used to transmit critical and sensitive information; such as social security and credit card numbers. Individuals assume full responsibility for their actions.

Coverage

UST's Wireless Network is currently installed throughout the majority of the campus (see wireless coverage map). IP tunneling is unavailable at this time and so users may need to reconnect when traveling from building to building. This is subject to change as the requirements of the users are continuously assessed. IT must approve all wireless access points across campus.

Access

Access to the UST-Admin network will be subject to approval by IT and considered on a case by case basis. Students, Staff, and Faculty will need to authenticate after joining the SSID of choice by opening a browser to be directed to the login page. Public connectivity, at this time, is accessible only when UST-Guest is broadcasted. By connecting any of the UST wireless networks you agree to the terms of use addressed in this policy and the Acceptable Use Policy.



Security

Wireless Networks are insecure. The security features of open WEP (Wired Equivalency Protocol) are flawed and allow for eavesdropping or "sniffing" of wireless traffic to potentially capture all traffic that is not encrypted with a third party product.

Eavesdropping on any UST network communication (wired or wireless) is illegal and a violation of the UST Acceptable Use and Wireless Usage policies. All violations will result in disciplinary action.

All computers connected to the UST network whether owned by the employee, student, or UST, must be running approved anti-virus software with the latest virus updates.

For security and network maintenance purposes, IT may monitor individual equipment, or wireless network traffic at any time. UST reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

IT has the authority to disconnect any device from the wireless network that violates the practices set forth in this policy or any other related policy. It is the responsibility if the user to be knowledgeable of the information set forth in such policies.

All Authorized Users, Guests and Students are responsible for the following:

- Adhering to established networking guidelines and policies.
- Implementation of security software (antivirus, firewalls), patches and protocols on all equipment used to access the UST Wireless Network.
- Compliance with all university policies and procedures and local and state laws pertaining to the security of sensitive and confidential data on the campus networks.
- Reporting known violations of the wireless network and all related equipment to IT.
 Violations

Any violations of the rules put forth in this policy may result in the following disciplinary actions being taken by the University:

- Limiting of a person's access to some or all of the university resources.
- Initiation of disciplinary actions by UST up to and including, but not limited to, termination of employment.
- Criminal prosecution under state and federal laws.