Tomball ISD Wireless Access Policy

The biggest security related problem with wireless networks is that they transmit potentially sensitive information over the airwaves. This means that the information flowing across the network can be intercepted by anyone within range who has a laptop equipped with a wireless network card. Likewise, wireless access points provide a way for hackers to enter your network without having to deal with the constraints normally associated with an Internet based attack. As such, wireless networks can pose a huge threat to a network's security unless you follow Tomball ISD's Wireless Access Policy.

Purpose and Scope

The goal of this policy is to protect Tomball ISD's technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to our public image. All users employing wireless methods of accessing District technology resources must adhere to District defined processes for doing so, using District approved access points. Unauthorized access to the wireless network is not allowed.

Wireless networks are not a replacement for a wired network. As the District's wireless network is an extension to the existing wired network. Wireless access should not be used for work sessions that require the transfer of large amounts of data (e.g., backups or file downloads) or for access to sensitive organizational data.

The following policy is complementary to any previously implemented policies dealing specifically with network access and remote access to the enterprise network.

Supported Technology

Tomball ISD uses the 802.11(a,b,g,n) protocols as its wireless network standard, transmitting at the 2.4 and 5GHz radio frequency spectrum, with the intention of delivering speeds of up to 160 Mbps to mobile and wireless devices.

In order to provide wireless access to authorized users, the Technology Department must install "access points" in and around the district. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g. PDA, laptop, etc.), which then converts the radio signal back to a digital format the mobile device can use.

Keep in mind that several categories of devices use radio frequencies in the same range as 802.11(a,b,g,n) wireless Ethernet and therefore other devices using the same frequencies may disrupt wireless communications. Devices such as cordless phones, microwave ovens, and personal network devices using Bluetooth technology may interfere. These interferences can be intermittent and very difficult to diagnose. The Technology Department will make every effort to resolve frequency conflicts between wireless access points; however, the Technology Department will not be responsible for resolving problems resulting from non-network wireless devices.

"Rogue" access points are antennas that are installed without the knowledge or permission of the Tomball ISD, used by individuals to gain illegal access to the District's network.

Tomball ISD supports the following devices and equipment for accessing our network and systems wirelessly:

- Access Points installed by the Technology Department
- Aruba client devices
- Laptop computers using Windows 2000 and XP operating systems and above.

Granting Access to Wireless Network

Access to and use of computing resources is available to all users who enter Tomball ISD. All Tomball ISD equipment will be updated with the proper security codes to automatically connect to the Tomball ISD Wireless Network; however, there may be times when you need to access the Tomball ISD Wireless Network for guest coming into Tomball ISD for a presentation.

TISD has created a TISD-PUBLIC SSID for guest to use when needing access to our wireless network. The TISD-PUBLIC Wi-Fi is an unsecured network that is separated from the TISD network for security reasons. Users do not need a password to access this Public Network.

Policy and Appropriate Use

1. All wireless access points within the District's firewall must be approved and centrally managed by the Tomball ISD's Technology Department. The addition of new wireless access points within campus facilities will be managed at the sole discretion of Technology. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment on campus premises, are strictly forbidden.
2. The Technology Department will occasionally conduct sweeps of the wireless network to ensure there are no rogue access points present.
3. The Technology Department reserves the right to turn off without notice any access point connected to the network that it feels puts the District's systems, data, and/or users at risk.
4. All wireless clients and devices are required to be fully patched and free of viruses. The user shall update applications as required, and will not reconfigure them in any way. 802.11 access point broadcast frequencies and channels shall be set and maintained by the Technology Department. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.
5. All computer equipment and devices used to connect to the District's network must display reasonable physical security measures. Users are expected to secure their District-connected devices when they are physically at their machines as well as when they step away.
6. Wireless access users agree to immediately report to Tomball ISD's Technology Department any incident or suspected incidents of unauthorized access point installation.
7. Use of the wireless network is subject to the same guidelines as the Tomball ISD's Acceptable Use and Internet Safety Policy.
8. Any questions relating to this policy should be directed to the Technology Department.

Policy Non-Compliance

Failure to comply with the Wireless Access Policy may result in the suspension of wireless access privileges and possible disciplinary action.