# 29.01.03.H0.14 Network/Wireless Access

Approved: April, 2014
Next Scheduled Review: April, 2019

## Procedure Statement

The information resources network infrastructure in Texarkana, Texas is provided by Texas A&M University-Texarkana for tenants of University facilities. It is important that the infrastructure, which includes media, active electronic equipment (i.e., switches, hubs, routers, etc.) and supporting software, be able to meet current performance requirements while retaining the flexibility to allow emerging developments in high speed networking technology and enhanced user services. The purpose of the Texas A&M University-Texarkana network access procedure is to establish the process for the access to the network infrastructure.

## Reason for Procedure

Required by Texas Administrative Code, Chapter 202.

This procedure applies to University information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this procedure is to provide a set of measures that will mitigate information security risks associated with Network and wireless access. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code, Chapter 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).

The intended audience for this procedure includes, but is not limited to, all information resources data/owners, users, management personnel, students and system administrators.

## Definitions

**Information Resources (IR):** the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

**Owner of an Information Resource:** an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

**Information Security Officer (ISO):** responsible for administering the information security functions within Texas A&M University-Texarkana and reports to the Information Resources Manager (IRM).

**Mission Critical Information:** information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

**Anonymous write capability:** the ability of people to save (on Texas A&M University-Texarkana computers) information they create without their identity being known (to system administrators).

**Anonymously originating network traffic:** causing a (Texas A&M University-Texarkana) computer system to send traffic via the network where the custodian/owner is not known.

## Procedures and Responsibilities

1. Network aggregation devices (e.g., hubs, switches, routers) shall not be connected to network infrastructure without prior approval by Information Resources.

2. Management of network addresses and name space may be delegated to system administrators. Users are permitted to use only those network addresses issued to them by their designated system administrator.

3. Network scans and network vulnerability scans of devices attached to the Texas A&M University-Texarkana network as well as the appropriate remediation are occasionally necessary to ensure the integrity of Texas A&M University-Texarkana computing systems. Network scans and network vulnerability scans may only be conducted by University employees designated by the organizational unit head responsible for the information resource.

4. Individuals controlling right-to-use for systems attached to the network infrastructure will ensure only authorized persons are granted access.

5. Allowing anonymous write capability to University systems or anonymously originating network traffic requires permission from the Department of Information Technology.

6. Users shall not alter University-owned network hardware in any way.

7. Wireless networking is available on the Texas A&M University-Texarkana campuses.
   7.1 The Wireless SSID used for the Texas A&M University-Texarkana Wireless network is TAMUTwlan. Use of this SSID for an unrelated network is forbidden.

7.2 Wireless networking is generally available within academic and administrative buildings.

7.3 Areas adjacent to covered buildings may have some "bleed-over" wireless coverage, but this coverage is not guaranteed.

7.4 Wireless access is available in the residence hall.

7.5 Wireless access is not provided off-campus in any location.

8. Departments and individuals must not install their own wireless access points.

8.1 Wireless access points include computers that have both wired and wireless interfaces that are configured to operate as a wireless router or wireless bridge.

8.2 Access points within offices may be removed by the Infrastructure team.

8.3 Access points within residence halls may cause the wired network interface in the room to be disabled. The director of residence life may establish additional disciplinary procedures.

9. Access to the wireless network is controlled through the campus Active Directory.

9.1 Users must login to use the wireless network. The wireless network does not support devices that cannot perform a web-based authentication. This disallows the use of devices such as video game consoles and WiFi VOIP devices.

9.2 Current faculty and staff will have accounts with permission to login to the wireless network.

9.3 Current students (students who are enrolled in the current semester, including mini-semesters) will have accounts with permission to login to the wireless network.

9.4 Guest access is provided for conferences and similar meetings. The organizer should contact the IT Help Desk for details as part of planning the event.

9.5 Access to the wireless network is terminated upon the completion of the current semester for students, upon termination of employment for faculty and staff, and after the end of the event for a conference.

10. Access from the wireless network may be restricted.

10.1 Access to TAMUT Information Resources is restricted to the HTTP and HTTPS protocols only.

10.2 Access to TAMUT Information Resources using other protocols requires the use of the VPN client. Instructions on using or installing the VPN client are available from the IT Support Center.

10.3 Access to other protocols, such as FTP, SSH, etc. is permitted to Internet resources.

10.4 Access to certain protocols and services is blocked completely.

10.5 Access restrictions may be changed as the design of the network changes.

11. Intentionally disrupting or attempting to disrupt the wireless network is not permitted.

11.1 Certain devices may interfere with wireless networks, as allowed by FCC regulations, including microwave ovens. This interference cannot be prevented.

11.2 Some building designs prevent or prohibit wireless coverage. Where possible, coverage has been augmented, but wired connections should be preferred in these areas.

## Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

## Contact Office

Department of Information Technology
903-223-3084