**Network Use Policy UPPS No. 04.01.05**

**Issue No. 9**

 **Effective Date: 10/07/2022**

**Next Review Date: 09/01/2024 (E2Y)**

**Sr. Reviewer: Associate Vice President for Technology Resources**

**POLICY STATEMENT**

Texas State University is committed to establishing appropriate use of information resources for the university community.

1. **BACKGROUND INFORMATION**

01.01 The purpose of this policy is to assure the reliability, security, integrity, and availability of the telecommunications network infrastructure at Texas State University. This policy documents practices and responsibilities associated with the administration, maintenance, expansion, and use of the university network in order to:

1. provide reliable intranet and internet communications for the efficient conduct of university operations;
2. assure that network usage is authorized and consistent with the university’s mission; and

c. protect the confidentiality, integrity, and availability of university information that traverses the university network.

01.02 No individual or university entity is permitted to independently deploy network devices that extend the university network, or secure or isolate parts of the institutional network, except as stipulated under this policy’s provisions.

01.03 The university’s Technology Resources department is charged with overall responsibility for proper deployment and management of a fully monitored and protected network communication service, including:

a. all network infrastructure elements including switches, routers, and

wireless access points; and

b. channel and spectrum coordination for all wireless access points.

01.04 The Information Security Office and Student Business Services must authorize in writing the provisioning of wired or wireless network connectivity before any application or service subject to the Payment Card Industry Data Security Standard (PCIDSS) is connected to the network.

01.05 To optimize their accessibility, usability, security, and privacy, all electronic and information resources developed or procured for use within the university network shall comply with the applicable provisions of [Texas Administrative Code, Chapter 213, Subchapter C, §213.30 – §213.37](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=213&sch=C&rl=Y), dealing with the accessibility, usability, and compatibility of electronic and information resources in institutions of higher education.

01.06 Only the vice president for Information Technology, or designee, may grant exceptions or exemptions to this policy.

**02. RELATED DOCUMENTS**

02.01 [UPPS No. 04.01.01](https://policies.txst.edu/university-policies/04-01-01.html), Security of Texas State Information Resources

02.02 [UPPS No. 04.01.02](https://policies.txst.edu/university-policies/04-01-02.html), Information Resources Identity and Access Management

02.03 [UPPS No. 04.01.07](https://policies.txst.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources

02.04 [UPPS No. 04.01.08](https://policies.txst.edu/university-policies/04-01-08.html), Texas State Domain Name and URL Policy

02.05 [UPPS No. 04.01.09](https://policies.txst.edu/university-policies/04-01-09.html), Server Management Policy

02.06 [UPPS No. 04.01.11](https://policies.txst.edu/university-policies/04-01-11.html), Risk Management of Information Resources

**03. DEFINITIONS**

03.01 Terms included in this policy have the meaning ascribed in the [Information Security Glossary](https://infosecurity.txst.edu/work/information-security-glossary.html) if included in the glossary and not explicitly defined otherwise.

03.02 Access Point – an electronic device that serves as a common connection point for devices seeking to use RF waves to connect to a wired network. Wireless access points provide shared bandwidth such that as the number of users connected to an access point increases, the bandwidth available to each user decreases.

03.03 Application Administrator – an individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of a software application or service that is accessed by users over the university network (may also be a server administrator, see Section 03.12). The application administrator role is analogous to the information system custodian role, as defined in [UPPS No. 04.01.11](https://policies.txst.edu/university-policies/04-01-11.html), Risk Management of Information Resources.

03.04 Device – any hardware component involved with the processing, storage, or forwarding of information making use of the institutional information technology infrastructure or attached to the institutional network. These devices include, but are not limited to, laptop computers, desktop computers, servers, and network devices such as routers, switches, wireless access points, and printers. Devices may have wired and wireless connectivity to the institutional network.

03.05 Dynamic Host Configuration Protocol (DHCP) – facilitates the temporary assignment of network addresses to devices from a pool of available addresses allowing the university to reuse addresses when devices no longer need them. DHCP is the predominant alternative to permanent, static network address assignment.

03.06 Extend the Network – connecting a device other than a single endpoint to a segment of the university network (most often a network port). For these purposes, an endpoint is defined as a device (e.g., a computer) that has no other network connections, physical or virtual, other than its physical link to the network port. Devices and other technologies that extend the network include hubs, bridges, switches, routers, firewalls, wireless access points, wireless extenders and repeaters, Network Address Translation (NAT) devices, Virtual Private Network (VPN) servers, and other information resources configured to provide any of these functionalities.

03.07 Interference – degradation of the network communication signal due to electrical pulses or electromagnetic radiation from an external source.

03.08 Internet – the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

03.09 Intranet – a computer network, especially one based on internet technology, that the institution uses for its own internal (and usually private) purposes and that is closed to outsiders; a generic name for the university network.

03.10 Network Address – a unique number associated with a device’s network connection used for the routing of traffic across the internet or another network. Also known as Internet Protocol Address or IP Address.

03.11 RESidential NETwork (ResNet) – the portion of the university network that serves university-owned and operated residence halls and apartment complexes. Because the vast majority of devices connected to the ResNet are personally owned and not under direct university management, special provisions are necessary to protect the university network against threats such systems could introduce (see Section 06.).

03.12 Server – a computer that provides a specific type of service on behalf of another computer or computer user (i.e., a client). Examples include a file server that stores and manages access to files, a web server that facilitates access to websites and pages, and a name server that maps user and computer names to machine and network addresses.

03.13 Server Administrator – an individual designated by the server owner as principally responsible for performing server management functions, including the installation, configuration, security, ongoing maintenance, and registration of the server (may also be an application administrator, see Section 03.02). The server administrator role is analogous to the information system custodian role, as defined in [UPPS No. 04.01.11](https://policies.txst.edu/university-policies/04-01-11.html), Risk Management of Information Resources.

03.14 Service Set Identifier (SSID) – the name of a wireless network, or more specifically, a set of characters that identify a specific wireless network, as defined in the [IEEE 802.11](https://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php) standards.

03.15 System Compromise – any device that is no longer entirely under its owner's control. Two major sources of compromise are:

a. infection by a worm, virus, Trojan horse, ransomware, or other malware; and

b. exploitation of an operating system or application vulnerability by another user giving that user remote control of the computer.

03.16 User – an individual, process, or automated application authorized to access an information resource in accordance with federal and state law, institution policy, and the information owner's procedures and rules.

03.17 University Network – the data and communications infrastructure at Texas State. It includes the campus backbone, various local area networks (such as the ResNet), and all equipment connected to those networks. It includes the wired and wireless networks. Also known as the institutional network.

03.18 Wireless Network – that part of the university network infrastructure that uses electromagnetic waves (per [IEEE 802.11](https://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php) standards) instead of copper or fiber optic cable to connect computing and communication devices to the rest of the university network and beyond.

**04. GENERAL PROCEDURES**

04.01 All devices connected to the Texas State network (wired or wireless) must support the university mission. The integrity, security, and proper operation of the university network require an orderly assignment of network addresses and the correct configuration of devices attached to the network. Network access, performance, and security are put at risk when devices are introduced into the network environment without appropriate coordination. To mitigate this risk, Technology Resources will manage all connections to the university network with due consideration for accessibility, performance, privacy, and security.

04.02 Technology Resources will coordinate the connection and network address assignment of any and all devices on the university network. Other departments and individual users may not install, alter, extend, or re-transmit network services in any way. Departments and individual users are prohibited from attaching or contracting with a vendor to attach equipment such as routers, switches, hubs, firewall appliances, wireless access points, VPN servers, network address translators, proxy servers, and dial-up servers to the university network without prior authorization from Technology Resources. Technology Resources may disconnect and confiscate any unauthorized network device, including wireless routers and access points. Software firewalls (i.e., host-based firewalls) on endpoints are permitted, as are printers, scanners, and similar peripheral devices if directly connected as a peripheral device to a desktop or notebook computer. Technology Resources reserves the right to monitor and audit individual devices, systems, and general network traffic to ensure compliance with this and other university policies.

04.03 The use of devices connected to the university network is accompanied by certain responsibilities. Specifically, all users are required to perform timely updates of applications, operating systems, and malware protection software to minimize risks of system compromise. The Division of Information Technology provides products and services for achieving such updates for university-managed devices.

04.04 The wired component of the university network is unencrypted. Server and application administrators that use this network to transmit sensitive or confidential information are responsible for the security of that information as it traverses the network. Examples of available protections include encrypted protocols such as TLS, IPSec, and SSH. The Information Security Office must be contacted for assistance in implementing the necessary protective measures (see Section 02.08 of [UPPS No. 04.01.11](https://policies.txst.edu/university-policies/04-01-11.html#section.02.08), Risk Management of Information Resources, for descriptions of sensitive and confidential information).

04.05 The university requires authorization for servers connected to the university network. To satisfy this requirement, Information Technology employs a variety of methods and tools to discover both planned and actively connected servers requiring registration, including:

1. network scanning and penetration testing;
2. network performance monitoring and anomaly investigation;
3. annual information security risk assessments;
4. notification from various sources of planned or completed server procurements;
5. collaboration in the server acquisition process with acquiring departments;
6. collaboration with campus construction entities in the design of facilities that require network connectivity;
7. reports of suspicious system activity from internal and external sources; and
8. other automated and manual methods and tools as they become available and prove effective.

Prior to authorization, the Information Security Office will facilitate an information resources security assessment to ensure compliance with state and university standards and best practices. For registration and assessment details, see the [Information Security Office Services website](https://infosecurity.txst.edu/services-tools/security-services.html).

04.06 A department’s administrative head is responsible for designating a server administrator for each server. The server administrator will collaborate with the Information Security Office and Technology Resources, as necessary, to:

a. receive authorization to operate the server from the Information Security Office;

b. protect the server against exploitation of known vulnerabilities. The Information Security Office and Technology Resources provide guidance for achieving such protection in its [Server Management Technical and Security Standards and Procedures](https://infosecurity.txst.edu/services-tools/security-services/server-management.html) and [[[[Server Administration Guidelines](http://itac.txst.edu/support/servers/server-admin-guidelines)](http://itac.txstate.edu/support/servers/server-admin-guidelines)](http://itac.txstate.edu/support/servers/server-admin-guidelines)](http://itac.txstate.edu/support/servers/server-admin-guidelines). Servers must comply with the provisions in this document any time they are connected to the university network. These standards and procedures will change over time to address new and evolving threats, so server administrators should refer back periodically for updates;

c. address and resolve security problems identified with any device for which they are responsible. The Division of Information Technology provides training, consulting, and problem resolution services;

d. utilize the protection benefits available through the university’s network edge protection mechanisms (e.g., firewall and intrusion prevention systems);

e. accommodate risk assessments, vulnerability scans, and penetration tests of their server by the Information Security Office and take steps to mitigate the risks identified by these procedures; and

f. immediately report system compromises and other security incidents in a timely manner to the Information Security Office at 512.245.HACK (4225) or infosecurity@txst.edu.

04.07 DHCP is the standard and preferred method for assigning IP addresses to campus devices. Departments or users desiring a static IP address may have to demonstrate why DHCP is inadequate for their purposes. Those denied static IP addresses may appeal to the director of Network Operations and then to the associate vice president for Technology Resources, whose decision is final. Technology Resources reserves the right to change static IP addresses periodically to address new or modified university requirements and will notify static IP address users in advance of pending changes to those addresses.

04.08 Virtually all rooms and meeting spaces at Texas State are equipped with wired or wireless connectivity. Nevertheless, facility reservations do NOT necessarily include the right to use the university network for any and all purposes. Consistent with [UPPS No. 04.01.07](https://policies.txst.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources, the university cannot guarantee support of outbound streaming of audio or video by reserving parties.

Departments that accept facility reservation requests from external parties shall ascertain the party’s need for outbound audio or video transmissions and consult with the associate vice president for Technology Resources, or designee, about that need. To assure compliance with this provision, departments that administer building or room reservations shall include the following (or similar) statement on all reservation applications and request forms:

“Outbound streaming of audio or video is not permitted from this facility without advance notice and consultation. The reserving party declares that it - DOES / DOES NOT (circle one) - wish to stream audio or video from this facility.”

**05. WIRELESS NETWORKING PROCEDURES**

* 1. The university provides a secure wireless network for students, faculty, and staff, as well as various secure and unsecure networks to support visitors and special events. Users with a Texas State NetID should use the secure network and avoid using the unsecure visitor network and other special purpose and event networks.

05.02 Consistent with the provisions of [UPPS No. 04.01.11](https://policies.txst.edu/university-policies/04-01-11.html#section.02.04), Risk Management of Information Resources, users are expected to use the secured wireless network when transmitting sensitive or confidential information, regardless of the application or service to which they are connecting.

05.03 The university operates both wired and wireless networks, which complement each other. The wireless networks facilitate network connectivity for outdoor and roaming users and in locations that prove difficult or costly to reach with traditional, wired connections as well as connectivity for mobile devices with no wired network interface. The wired networks provide consistent, high-quality service for high-bandwidth or latency-intolerant applications, such as streaming media, IP telephony, online gaming, and large file transfers. Users should choose the type of network connection that best meets their specific needs.

05.04 Wireless bandwidth is shared by everyone connected to a given access point. As the access point’s user numbers increase, available bandwidth per user decreases. Thus, departments and users should carefully consider the user-to-access point ratio and the characteristics of the expected transmissions and consult with Technology Resources prior to designing or implementing computer labs, classroom facilities, office spaces, or other new, renovated, or repurposed spaces that rely on wireless access for their network connectivity. Likewise, departments and individual users with wired connections to their desktop computers may not abandon those connections simply because wireless is available in their location.

05.05 The university’s wireless networks utilize the unlicensed RF bands allocated by the FCC for wireless network data transmission. Transmissions from other devices (e.g., cordless phones and microwave ovens) that use these frequencies can seriously degrade network performance. The university has the authority to regulate unlicensed 2.4GHz and 5GHz RF bands on its premises and, through Technology Resources, may restrict the use of 2.4GHz or 5GHz RF devices it believes pose a disruption to the wireless network in university-owned or managed spaces.

05.06 Consistent with the provisions of [UPPS No. 04.01.02](https://policies.txst.edu/university-policies/04-01-02.html), Information Resources Identity and Access Management, only the owner of an individual Texas State NetID account is authorized to know and use the password to that account, and account owners are responsible for all computing and network activities attributable to that account. As such, the use of an individual user’s account to connect devices intended for shared or infrastructure purposes to the wireless network is prohibited; instead, owners and custodians of such devices should contact Technology Resources to determine appropriate, alternative methods of establishing connectivity.

**06. PROCEDURES FOR NETWORK USE IN RESIDENCE HALLS**

06.01 ResNet is the name given to the portion of the university network that serves university-owned and operated residence halls and apartment complexes. The university provides at least one active wired or wireless network connection per residence hall room or apartment in addition to wireless network access.

Because most devices connected to the ResNet are personally owned and not under direct university management, the special provisions contained in this section are necessary to protect the university network against threats such systems may introduce. The above notwithstanding, all ResNet users are subject to all other sections of this policy, as well as all other university policies that govern the use of information resources at Texas State.

06.02 ResNet users are responsible for the security of the networked devices they connect to the ResNet. Failure to maintain secure computing devices may result in diminished or suspended network access and repeated failures may subject the user to further disciplinary action.

06.03 The university assumes no responsibility for a user’s loss of time, data, or other loss due to unavailable or diminished ResNet services. Network connectivity may be intentionally disrupted at any time as necessary to safeguard the university, its constituents, or its information resources.

06.04 The university enforces the following network access policies for all ResNet connections:

1. users must keep their operating systems and applications up to date with all security patches; and
2. users must install, activate, and configure malware protection software to maintain up-to-date definitions.

06.05 In addition to the restrictions identified in [UPPS No. 04.01.07](https://policies.txst.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources, the university strictly prohibits users from engaging in the following activities on the university ResNet:

1. attempting to circumvent the authentication required for ResNet connections;
2. eavesdropping or capturing packets intended for other systems;
3. scanning other systems for open ports, open file shares, or other vulnerabilities;
4. unauthorized use of or access to other users’ devices without permission of the device owner;
5. operating any server or network service available to the public or to other users of the university network, including:
	1. video game servers (see Section 06.06);
	2. music or video servers (e.g., MP3, MPEG);
	3. peer-to-peer (P2P) services (e.g., BitTorrent);
	4. dynamic address assignment services (e.g., DHCP);
	5. electronic mail services (e.g., SMTP);
	6. file transport services (e.g., FTP);
	7. domain name translation services (e.g., DNS);
	8. network chat services (e.g., IRC); and
	9. web services (e.g., HTTP).
6. installing routers or any devices that provide routing functionality including wireless routers, VoIP devices with built-in routers, or Network Address Translation (NAT) devices even if the routing, NAT, or DHCP functions have been disabled;
7. using a host name that incorporates offensive or profane language or that makes the system appear university-owned and operated;
8. changing the Media Access Control (MAC) address to conceal the system’s identity or function; and
9. installing or enabling unauthorized software or hardware intended to facilitate remote access to devices or other components of the university network.

06.06 Online gaming consoles (e.g., XBOX, PlayStation, or Nintendo) may connect to the ResNet, but university support is limited to basic network connectivity. ResNet users should note that gaming consoles do not generally incorporate host firewalls, anti-malware protection, or other security features commonly available for general purpose personal computers with up-to-date operating systems. Consequently, ResNet users should utilize their gaming consoles solely for gaming, video streaming, and other, similar entertainment purposes and avoid the use of consoles for higher risk activities like web browsing. The use of gaming consoles in violation of this policy; [UPPS No. 04.01.07](https://policies.txstate.edu/university-policies/04-01-07.html), Appropriate Use of Information Resources; or any other university policy may result in revocation of gaming privileges and other progressive disciplinary action.

Similarly, gaming consoles are primarily designed for personal, consumer use on residential networks, and many online gaming services (e.g., match-making servers for online games) may rely on certain networking protocols that are incompatible with enterprise networks from a technological perspective or because they present an unacceptable level of risk to the rest of the enterprise’s network. As such, basic network connectivity afforded to the ResNet for online gaming may not fully accommodate all online gaming consoles, online gaming services, online games, or related features.

**07. PROCEDURES FOR RESPONSE TO THREATS AND POLICY VIOLATIONS**

07.01 The Information Security Office or Technology Resources will disconnect a device posing an immediate threat to the university network in order to isolate the intrusion or problem and minimize risk to other systems until the device is repaired and the threat is removed. In coordination with administrative departments and law enforcement, the Information Security Office and Technology Resources will investigate any incident involving unauthorized access or improper use of the university network. Devices involved in these and other incidents will remain disconnected from the university network until the user, owner, or server administrator brings the device into compliance with all relevant policies and standards. The Information Security Office and Technology Resources will attempt to notify appropriate departmental personnel when disconnecting departmental devices from the network under this provision.

07.02 The Division of Information Technology may disconnect devices involved in repeated incidents for longer periods as required to reduce security risks to an acceptable level. The Information Security Office may require the responsible server administrator to demonstrate compliance with [UPPS No. 04.01.09](https://policies.txst.edu/university-policies/04-01-09.html), Server Management Policy and the [Server Management Technical and Security Standards and Procedures](https://infosecurity.txst.edu/services-tools/security-services/server-management.html) through an audit review or other assessment of the offending device and any other devices for which the administrator is responsible.

07.03 Texas State cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations. The university will file criminal complaints against users who access or utilize the university network to conduct any criminal act.

**08. REVIEWERS OF THIS UPPS**

08.01 Reviewers of this UPPS include the following:

Position Date

Associate Vice President for September 1 E2Y

Technology Resources

Chief Information Security Officer September 1 E2Y

Director, Network Operations September 1 E2Y

Vice President for Information September 1 E2Y

Technology

**09. CERTIFICATION STATEMENT**

This UPPS has been approved by the following individuals in their official capacities and represents Texas State policy and procedure from the date of this document until superseded.

Associate Vice President for Technology Resources; senior reviewer of this UPPS

Vice President for Information Technology

President