01. POLICY STATEMENTS

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

a. provide reliable Intranet and Internet communications for the efficient conduct of University business;

b. 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 component is permitted to independently deploy network devices that extend the University Network, or secure or isolate parts of the University Network, except as stipulated under this policy’s provisions. 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 all infrastructure elements, network address assignments, and radio frequency (RF) spectrum usage. Only the vice president for Information Technology or a designee may grant exceptions or exemptions to this policy.

01.03 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, Rules §213.30 – §213.37, dealing with the accessibility, usability, and compatibility of Electronic and Information Resources in Institutions of Higher Education, commonly known as TAC 213.
02. RELATED DOCUMENTS

UPPS 04.01.01, Security of Texas State Information Resources
UPPS 04.01.07, Appropriate Use of Information Resources
UPPS 04.01.08, Texas State Internet Domain Name Policy
UPPS 04.01.09, Server Management Policy

03. DEFINITIONS

03.01 Access Point – an electronic device that serves as a common connection point for devices seeking to use radio frequency 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.

03.02 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 03.12).

03.03 Device – any hardware component attached to the University Network to process, store, or transmit information. Examples of devices include laptop computers, desktop computers, servers, and network devices such as routers, switches, wireless access points, and printers.

03.04 DHCP (Dynamic Host Configuration Protocol) – 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.

03.05 Extend the Network – connecting a device other than a single end-system to a segment of the University Network (most often a data jack). For these purposes, an end-system 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 data jack. Devices that extend the network include but are not limited to hubs, bridges, switches, routers, firewalls, NATs, VPN servers, or computers configured to provide any of this functionality. Extending the network does NOT include the use of software solutions such as Microsoft Windows Remote Desktop to connect to machines on the University Network from remote locations.

03.06 Interference – degradation of network communication signal due to electrical pulses or electromagnetic radiation from an external source.
03.07 Internet – a standards-based, global system of interconnected networks that utilizes Transmission Control Protocol / Internet Protocol (TCP/IP) for data representation, signaling, authentication, and error detection.

03.08 Intranet – a private computer network that uses Internet technologies and standards to securely share an organization’s information with the organization’s constituents; a generic name for the University Network.

03.09 Network Address (aka Internet Protocol Address or IP Address) – a unique identifier assigned to a network-connected device that is used to route network transmissions to their intended destinations on the Internet or Intranet.

03.10 ResNet (or RESidential NETwork) – that 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 of this UPPS).

03.11 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 Web sites and pages, and a name server that maps user and computer names to machine and network addresses.

03.12 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 03.12).

03.13 SSID (Service Set Identifier) – 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 standards.

03.14 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 or Trojan horse; and
   b. exploitation of an operating system or application vulnerability by another user giving that user remote control of the computer.

03.15 User – An individual who utilizes an information technology device or service.
03.16 **University Network** – the data and communications infrastructure at Texas State University-San Marcos. It includes the campus backbone, various local area networks (LANs, such as the ResNet), and all equipment connected to those networks. It includes the wired network as well as both the secure (encrypted) and open (un-encrypted) wireless networks.

03.17 **Wireless Network** – that part of the University Network infrastructure that uses electromagnetic waves (per IEEE 802.11 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 GUIDELINES**

04.01 All devices connected to the Texas State University 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 shall manage all connections to the University Network with due consideration for accessibility, performance, privacy, and security.

04.02 Technology Resources shall 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, virtual private network (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. Personal software firewalls are permitted, as are printers, scanners, and similar peripheral devices if directly connected as a slave 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 virus protection software to minimize risks of system compromise. Technology Resources provides non-intrusive products and services for achieving such updates.
04.04 The wired component of the University Network is unencrypted. Server and application administrators that utilize this network to transmit sensitive or restricted and confidential information are responsible for the security of that information as it traverses the network. Examples of available protections include encrypted protocols such as SSL, IPSec, SSH, etc. Contact IT Security for assistance in implementing the necessary protective measures. (NB. Sensitive and restricted/confidential information are fully described in section 04.08 of UPPS 04.01.01, Security of Texas State Information Resources).

04.05 The university requires the registration of servers connected to the University Network. Following registration, IT Security will facilitate an information resources risk assessment to ensure compliance with State and University standards and best practices. For registration and assessment details, see: http://security.vpit.txstate.edu/tools.html.

A department’s administrative head is responsible for designating a server administrator for each server. The server administrator shall collaborate with IT Security and Technology Resources as necessary to:

a. register the server with IT Security.

b. protect the server against exploitation of known vulnerabilities. IT Security provides guidance for achieving such protection in its Server Management Technical and Security Standards and Procedures. Servers must comply with the provisions in this document anytime they are connected to the University Network. These Standards and Procedures will evolve 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. Both IT Security and Technology Resources provide training, consulting, and problem resolution services;

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

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

f. immediately report system compromises and other security incidents in a timely manner to IT Security at 512-245-HACK (4225) or itsecurity@txstate.edu.
04.06 DHCP (see definitions - Dynamic Host Configuration Protocol) 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 purpose. Those denied static IP addresses may appeal to the director of Infrastructure Services and then to the assistant 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.

04.07 Internet connectivity is ubiquitous across the campus. 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 01.04.13 (Policy Guidelines for the Use of Texas State Equipment by Outside Entities) and UPPS 04.01.07 (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 assistant vice president for Technology Resources or designee about that need. To assure compliance with this provision, departments that administer building or room reservations should 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

05.01 The University Network includes two separate wireless networks:

a. The open wireless network (broadcast SSID “TexasStateUniversity”) transmits all traffic “in the clear,” or unencrypted, and is restricted to use with web-based services. Such services include general Internet browsing, public email services such as Gmail and Hotmail, and Texas State Web-based applications like BobcatMail, CatsWeb, and TRACS. Non Web-based applications and services like SAPGUI, the ACCESS Menu, and Email and Calendaring using Outlook or Entourage are inaccessible via this network.
Users, services, and applications shall utilize a suitable encrypted protocol (e.g., https, IPSec, VPN, etc.) whenever they transmit sensitive or restricted and confidential information across the University Network. Similarly, users assume all responsibility for the security and privacy of any sensitive personal information that they transmit over this network and are strongly advised to avoid such transmissions unless encrypted protocols are used.

b. The secured wireless network (broadcast SSID “TexasStateWPA”) encrypts all traffic using Wi-Fi Protected Access (WPA2). To connect to this network, users must login, or authenticate, using their Texas State NetID and password. All Texas State services and applications, both Web-based and traditional, are accessible via this network. All users shall use the secured wireless network when connecting wirelessly to terminal/host or client/server applications and services, such as SAPGUI, the ACCESS menu, and Email and Calendaring using Outlook or Entourage.

05.02 Consistent with the provisions of UPPS 04.01.01, Security of Texas State Information Resources, users are expected to utilize the secured wireless network when transmitting sensitive or restricted and confidential information, regardless of the application or service to which they are connecting.

05.03 The University’s wireless networks are designed to supplement and enhance the wired network, not replace it. They are designed to facilitate network connectivity for outdoor and roaming users, and in locations that prove difficult or costly to reach with traditional wired connections. The wireless networks are not designed to provide the consistently high quality of service required by high-bandwidth or latency intolerant applications, such as streaming media, IP telephony, on-line gaming, and large file transfers.

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, the ratio of users to access points and the characteristics of the expected transmissions should be carefully considered. For this reason, departments and users shall consult with Technology Resources prior to designing or implementing computer labs or classroom facilities that rely heavily or exclusively 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 To mitigate risk, IT Security and Student Business Services must authorize the provisioning of wireless connectivity to any application or
service subject to the Payment Card Industry Data Security Standard (PCI DSS).

05.06 The university’s wireless networks utilize the unlicensed 2.4GHz and 5GHz radio frequency (RF) bands for data transmission. Transmissions from other devices (e.g., cordless phones, microwave ovens, etc.) 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 2.5 or 5GHz RF devices it believes pose a disruption to the wireless network in university owned or managed spaces."

06. NETWORK USE IN RESIDENCE HALLS

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

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 computing 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:
   a. Users must authenticate using their University NetID and password in order to establish a connection;
   b. Users must keep their operating systems and applications up-to-date with all security patches;
   c. Users must install, activate, and configure virus protection software to maintain up-to-date virus definitions.
06.05 In addition to the restrictions detailed in UPPS 04.01.07, Appropriate Use of Information Resources, users are strictly prohibited from engaging in the following activities on the University ResNet:

a. attempting to circumvent the authentication required for ResNet connections;
b. eavesdropping or capturing packets intended for other systems;
c. scanning other systems for open ports, open file shares, or other vulnerabilities;
d. operating any server or network service available to the public or to other users of the University Network, including:
   - video game servers (see section 06.06 for more about gaming);
   - music or video servers (e.g., MP3, MPEG);
   - peer-to-peer (P2P) services (e.g., LimeWire, BitTorrent);
   - dynamic address assignment services (e.g., DHCP);
   - electronic mail services (e.g., SMTP);
   - file transport services (e.g., FTP);
   - domain name translation services (e.g., DNS);
   - network chat services (e.g., IRC);
   - Web services (e.g., HTTP);
   - or similar functions.

e. installing routers or any device that provides 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;

f. using a host name that incorporates offensive or profane language or that makes the system appear university owned and operated;

g. changing the Media Access Control (MAC) address to conceal the system’s identity or function.

06.06 Online gaming consoles (e.g., Xbox, PS2, Wii, etc.) 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 purposes and avoid the use of consoles for higher risk activities like web browsing and Internet chat. The use of gaming consoles in violation of this policy, the University’s appropriate use policy, or any other university policy may result in revocation of gaming privileges and other progressive disciplinary action.

07. PROCEDURE FOR RESPONSE TO THREATS AND POLICY VIOLATIONS

07.01 IT Security 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, IT Security 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. IT Security and Technology Resources will attempt to notify appropriate departmental personnel when disconnecting departmental devices from the network under this provision.

07.02 IT Security and Technology Resources may disconnect devices involved in repeated incidents for longer periods as required to reduce security risks to an acceptable level. IT Security may require the responsible server administrator to demonstrate compliance with UPPS No. 04.01.09, Server Management Policy, and the Server Management Technical and Security Standards and Procedures through an audit review or other assessment of the offending device and any other devices for which the administrator is responsible. If a server administrator lacks the knowledge or training needed to comply with this policy, Technology Resources will assist the department in addressing the deficiency, including development of an appropriate training program.

07.03 Texas State cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations. Users are reminded that the University will file criminal complaints against those who access or utilize the University Network in the conduct of any criminal act.

08. REVIEWERS OF THIS UPPS

*08.01 Reviewers of this UPPS include the following:

<table>
<thead>
<tr>
<th>Position</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special Assistant to the Vice President</td>
<td>September 1 E2Y</td>
</tr>
<tr>
<td>for Information Technology</td>
<td></td>
</tr>
<tr>
<td>Information Security Officer</td>
<td>September 1 E2Y</td>
</tr>
<tr>
<td>Director, Infrastructure Services</td>
<td>September 1 E2Y</td>
</tr>
<tr>
<td>Assistant Vice President for Technology Resources</td>
<td>September 1 E2Y</td>
</tr>
<tr>
<td>Vice President for Information Technology</td>
<td>September 1 E2Y</td>
</tr>
</tbody>
</table>
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.

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

Vice President for Information Technology

President