01. POLICY STATEMENTS

01.01 The purpose of this policy statement is to assure the reliability, security, integrity, and availability of the telecommunications network infrastructure at Lamar Institute of Technology (LIT). This policy documents practices and responsibilities associated with the administration, maintenance, expansion, and use of the LIT network in order to:

a. provide reliable Intranet and Internet communications for the efficient conduct of Institutional business;
b. assure that network usage is authorized and consistent with the institution’s mission; and
c. protect the confidentiality, integrity, and availability of institutional information that traverses the LIT Network.

01.02 No individual or LIT component is permitted to independently deploy network devices that extend the LIT Network, or secure or isolate parts of the LIT Network, except as may be stipulated under the provisions of this policy. The LIT Technology Services 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. No exceptions or exemptions to this policy shall be granted without the express written approval of the Director of Computer Services or designee.

01.03 To optimize their accessibility, usability, security, and privacy, all electronic and information resources developed or procured for use within the LIT network shall comply with the applicable provisions of institutional, TSUS, and State mandate dealing with the accessibility, usability, and compatibility of electronic and information resources in Institutions of Higher Education.

02. RELATED DOCUMENTS

a. Appropriate Use of Information Technology Policy
b. Server Management Policy
c. Information Security Policy
d. Server Management Standards and Procedures

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 LIT Network (may also be a Server Administrator, see 03.11).

03.03 **Device** – any hardware component that can be attached to the LIT Network to process, store, or transmit information. Examples of devices include smartphones, MiFi devices, 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 a network address to a device from a pool of available addresses so that addresses can be reused 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 LIT 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 LIT 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 LIT 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 **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.

03.11 **Server Administrator** – an individual (including contractors and service providers) 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.

03.12 **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.

03.13 **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.

03.14 **User** – An individual who utilizes an information technology device or service.

03.15 **LIT Network** – the data and communications infrastructure at Lamar Institute of Technology. It includes the campus backbone, various local area networks (LANs), and all equipment connected to those networks including remote locations. It includes the wired network as well as both the secure (encrypted) and open (unencrypted) wireless networks.

03.16 **Wireless Network** – that part of the LIT 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 LIT Network infrastructure and beyond.

04. **GENERAL GUIDELINES**

04.01 All devices connected to the LIT Network (wired or wireless) must be associated with, and in support of, the mission of the institution. The integrity, security, and proper operation of the LIT 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, all connections to the LIT Network must be managed with due consideration for accessibility, performance, privacy, and security.
04.02 Technology Services shall coordinate the connection and network address assignment of any and all devices on the LIT 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 LIT Network without prior authorization from Technology Services. Technology Services 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 Services reserves the right to monitor and audit individual devices, systems, and general network traffic to ensure compliance with this and other LIT policies.

04.03 The use of all devices connected to the LIT Network, including institutional issued and personal laptops and wireless devices, 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 Services provides products and services for achieving such updates.

04.04 The wired component of the LIT Network is unencrypted. Server and application administrators that utilize this network to transmit sensitive or restricted/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 Technology Services for assistance in implementing the necessary protective measures.

04.05 All servers that deliver services across the LIT Network must be registered with Technology Services. Following registration, Technology Services will facilitate an information resources risk assessment to ensure compliance with State and institutional standards and best practices. For registration please contact the Technology Services help desk at (409) 839-2074 or helpdesk@lit.edu.

A department’s administrative supervisor is responsible for designating a server administrator for each registered server. The server administrator shall collaborate with Technology Services as necessary to:

a. protect server(s) against exploitation of known vulnerabilities. Technology Services provides guidance for achieving such protection in its Server Management Standards and Procedures. Servers must comply with the provisions in this document anytime they are connected to the LIT Network. These Standards and Procedures will evolve over time to address
new and evolving threats, so server administrators should refer back periodically for updates.

b. address and resolve security problems identified with any device for which they are responsible. Technology Services provides consulting and problem resolution services;

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

d. accommodate risk assessments, vulnerability scans, and penetration tests of their server(s) by Technology Services takes steps to mitigate the risks identified by these procedures;

e. immediately report system compromises and other security incidents in a timely manner to Technology Services help desk at (409) 839-2074 or helpdesk@lit.edu

04.06 DHCP (see definitions - Dynamic Host Configuration Protocol) is the standard and preferred method for assigning IP addresses to campus devices. Users desiring a static IP address may be asked to demonstrate why DHCP is inadequate for their purpose. Technology Services reserves the right to change static IP addresses periodically to address new or modified institutional requirements; users of static IP addresses will be notified in advance of pending changes to those addresses.

04.07 Internet connectivity is ubiquitous across the campus. Virtually all rooms and meeting spaces at LIT are equipped with wired or wireless connectivity. Nevertheless, facility reservations do NOT necessarily include the right to use the LIT Network for any and all purposes. Departments that administer facility reservations shall ascertain the reserving party’s need for network, audio, and video transmissions and consult with Technology Services should there be such a need. Outbound streaming of audio or video is not permitted from this facility without advance notice and consultation.

05. WIRELESS NETWORKING

05.01 The LIT Network includes two separate wireless networks:

a. The open wireless network 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 LIT Web-based applications like web mail and Banner self-service. Non
Web-based applications and services like Banner INB and network drives are inaccessible via this network.

b. LIT information classified confidential shall not be transmitted across this network without the use of a suitable encrypted protocol (e.g., https, IPSec, VPN, etc.) Similarly, users assume all responsibility for the security and privacy of any confidential personal information that they transmit over this network and are strongly advised to avoid such transmissions unless encrypted protocols are used.

05.02 The LIT wireless network is designed to supplement and enhance the wired network, not replace it. It is 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 network is 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.

05.03 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.

06. PROCEDURE FOR RESPONSE TO THREATS AND POLICY VIOLATIONS

06.01 Devices posing an immediate threat to the LIT Network will be disconnected from the network 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, Technology Services will investigate any incident involving unauthorized access or improper use of the LIT Network. Devices involved in these and other incidents will remain disconnected from the LIT Network until the user or server administrator brings the device into compliance with all relevant policies and standards. Technology Services will attempt to notify appropriate departmental personnel when devices in their department are disconnected from the network under this provision.

06.02 Devices involved in repeated incidents may be disconnected from the LIT Network for longer periods of time as required to reduce security risks to an acceptable and sustainable level. Server administrators will be required to demonstrate compliance with Server Management Policy, and security standards and procedures through an audit review or other assessment of the network-attached devices for which they are responsible. If a server administrator lacks
the knowledge or training needed to comply with this policy, Technology Services will assist the department in addressing the deficiency.

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