1.0 OVERVIEW AND PURPOSE

The purpose of this policy is to assure the reliability, security, integrity, availability, authenticity, and confidentiality of information on the data network infrastructure at Lamar University. The Lamar University central Information Technology Services Division (ITS), and more specifically Information Technology Infrastructure Services Department (ITIS), is charged with overall responsibility for properly deploying and managing a fully monitored and protected network infrastructure in accordance with TAC 202. 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. ensure the use of LUnet is authorized and in alignment with the university’s mission and initiatives
c. protect the confidentiality, integrity, and availability of university information that traverses LUnet

2.0 SCOPE

Network communication services encompass all infrastructure elements that include but are not limited to wireless and voice transmissions traversing the approved radio frequency (RF) spectrum. This policy applies to the methods and mechanics of data transmission as well as the logical assignment of IP addresses of equipment that traverse LUnet. All Lamar University departments, personnel, and third party contractors are subject to this policy.

3.0 DEFINITIONS

Access Point – Any piece of equipment that allows connectivity to network services via a radio frequency wireless connection. 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. These devices commonly provide adequate bandwidth for common network usage such as web and file services.

Device Administrator – an individual who is assigned by the “Device Owner” with principal responsibility for the installation, configuration, security, and ongoing maintenance of any type of device – be it, “User device” or “network device”, which attaches to or provides services through LUnet.
Device Owner – the department head charged with overall responsibility for the “User device” or “Networking device”, which is attached to LUnet. The device owner must designate an individual to serve as the primary device administrator.

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.

Domain Name System (DNS) and DNS services – hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet.

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 user device (e.g., a computer or printer) that has no other network connections, physical or virtual, other than its physical link to the data jack. Devices that extend the network include hubs, bridges, switches, routers, firewalls, or computers configured to provide any external network service other than for the sole use of the device itself.

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.

Intranet – a private computer network that uses Internet technologies and standards to share in a secure fashion an organization’s information with the organization’s constituents.

Information Resource – defined in §2054.003(7), government code and/or other applicable state or federal legislation as follows:

> Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.*

*Modification of this definition through state or federal legislation shall supersede the above.*

Information Resources of Lamar University include, but are not limited to:

- All components of the Lamar University information network, both physical and logical.
- Any device owned by Lamar University or used to connect to LUnet.
- These devices include computers (both stationary and mobile), printers, and communication devices.
• All software purchased by or used to support Lamar University.
• All electronic data, including email, and the storage media on which the data resides (both stationary and mobile).
• Lamar University credentials used to access licensed external resources.

Information Technology Services (ITS) – The Information Technology Services Division supports the IT needs of Lamar University.

Information Security Office (ISO) – responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected.

Information Technology Infrastructure Services (ITIS) – The department under ITS that has ownership of datacenter services, systems administration, telecommunication services, and network services.

Lamar Electronic Account (LEA) – A network account credential created by the university for “users” to access campus electronic resources.

(LUnet) Lamar University Network – the data and communications infrastructure at Lamar University. It includes the campus backbone, various local area networks (LANs), 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.

Network Address Assignment and Address Management – The process of delivering and assigning IP addresses to “user devices” and “network devices” using a centralized technology for LUnet.

Network Device – Used to facilitate the transmission of “user” data throughout the Lamar University campus using LUnet. Examples of network devices are network cabling, routers, switches, wireless access points, and in general, any non-endpoint device.

Security Operations Center (SOC) – The department under ITS that manages and is responsible for security issues, on an organizational and technical level which is led by the ISO.

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 standards.

System Compromise – any user device that is no longer entirely under the device owner or device administrator 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 user device.

User – An individual who utilizes an information resource device or service.
**User Device** – any hardware component attached to LUnet for use by a user to process, store, or transmit information. Examples of User devices include laptop computers, desktop computers, servers, scanners, and printers.

**TAC 202** – Texas administrative code for regulating information security standards.

**Wireless network** – that part of LUnet infrastructure that uses radio frequency signals (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.

### 4.0 POLICY

1. All devices connected to the university network (regardless of media type) must support the university mission and initiatives. The integrity, security, and proper operation of LUnet are the fundamental priorities of the CIO/VP of ITS and ITIS. [Part of that operation is the task of protecting these devices against unauthorized access, disclosure, modification or destruction. Network access, performance, and security are put at risk when devices are introduced into the network environment without appropriate coordination and compatibility verification.] ITIS shall manage all connections to LUnet with due consideration for accessibility, performance, privacy, compatibility, and security. Individuals or departments are NOT permitted to deploy any device or mechanism which would allow the extension or isolation of LUnet.

2. Lamar University ITS with ITIS owns and operates all IP addresses for LUnet. These include both public (internet routable) and private (non-internet routable) address spaces. The address designation for networks shall be determined by the purpose of the network towards supporting the university’s mission and initiatives. These addresses are commonly assigned by an ITS DHCP service, which dynamically assigns these addresses to individual user devices and network devices, when requested on LUnet. DHCP is the standard and preferred method for assigning IP addresses to campus user devices. Device owners or device administrators desiring a static (reserved) IP address may have to demonstrate why DHCP is inadequate for their purpose. Those denied static IP addresses may appeal to the Director of ITIS and then to the Chief Information Officer whose decision is final. ITIS reserves the right to change static IP addresses periodically to address new or modified university requirements. ITIS will notify statically addressed device owners or devices administrators in advance of pending changes to those addresses.

3. Lamar University ITS with ITIS owns and operates all root resolvers (DNS services) for LUnet (lamar.edu domain). These include forward and reverse resolvers. Campus departments may obtain sub domain delegations for their departments by contacting ITIS. These delegations may be hosted on the Lamar University ITS resolvers or department managed servers. Any such servers are subject to compliance with LU server management policy 10.03.01.

4. Lamar University ITS with ITIS shall coordinate the connection, the network address assignment and address management of all network devices, and user devices on LUnet. 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 network devices to LUnet without prior authorization from Lamar University ITS.

Network device equipment examples include but are not limited to:
- routers
- switches
- hubs
- firewall appliances
- wireless access points
- virtual private network (VPN) servers
- network address translators (NAT)
- proxy servers
- dial-up servers
- active/passive sniffer
- wiretaps or surveillance equipment

5. ITIS will disconnect a device posing an immediate threat to LUnet in order to isolate the intrusion or problem and minimize risk to other systems. Any user devices or network devices may be removed from LUnet if the traffic emanating from the device has been deemed a threat to the university or any of the other devices connected to LUnet. ITIS and SOC will disconnect devices involved in repeated incidents until it has been determined they are safe for reconnection to LUnet as required to reduce security risks to an acceptable level.

6. ITIS may disconnect and confiscate any unauthorized network devices. Personal software firewalls are permitted as long as these firewalls do not interfere with university services designed to assess security posture of connected devices. Network attached peripheral equipment such as printers, scanners, and similar devices are allowed where appropriate and with approval from Lamar ITS. ITIS reserves the right to monitor the traffic and audit state owned devices, systems, and general network traffic in accordance with Appropriate Use Policy number 10.01.01.

7. The use of user devices and network devices connected to the LUnet is accompanied by certain responsibilities. Users, device administrators, and device owners are accountable for their user device or network device connected to LUnet. Device owners are responsible for ensuring timely updates of applications, operating systems, and virus protection software to minimize risks of system compromise. [ITIS may provide non-intrusive products and services for achieving such updates for university owned equipment.]

8. The wired component of the LUnet is unencrypted. Device owner and device administrators that utilize this network to transmit sensitive, restricted, or confidential information are responsible for the security of that information as it traverses the network. Privacy of data traversing this network cannot be guaranteed. Examples of available protections include encrypted protocols such as SSL, IPsec, SSH, etc. Contact the SOC for assistance in implementing the necessary protective measures.

9. The university requires the registration of servers connected to LUnet by the device owner or device administrator. The guidelines for this are listed in Policy 10.03.01 Server Management
Policy. All unregistered public facing servers will be considered unauthorized devices and are subject to disconnection from LUnet by ITIS or SOC.

10. Metadata information about all university network traffic shall be logged and used for analysis towards improving performance of network services. Retention of these logs shall follow university retention guidelines unless superseded by state or federal laws.

11. Scanning, sniffing or capture of any part of network communications is strictly prohibited except for ITS personnel responsible for network and/or security operations. Exemptions can be granted with explicit written approval from the CIO / VP of ITS or their designee.

12. Lamar University ITS with ITIS reserves the right to segment internal network communications to optimize network flow within the campus network. These optimizations include but are not limited to interior segmentation, firewalls, traffic shaping and blocking of traffic.

13. Lamar University ITS with SOC may scan both secured and insecure network communication protocols for detection and suppression of malware for prevention and mitigation of risk from network-based malware.

14. Lamar University ITS with ITIS in conjunction with the office of ISO shall establish a network perimeter as mandated by TAC 202.75 and deploy technology components including but not limited to DMZ, firewall, intrusion detection or prevention system, routers, application firewalls, malware scanners, DLP systems. ITIS may deploy tools, technology and services designed for device recognition in conjunction with user recognition to determine authentication and authorization grants for users of LUnet.

15. WIRELESS NETWORKING:

   a. All wireless networks provided by the university operate in currently unlicensed spectrum and are hence subjected to interference from competing or neighboring networks and reliability cannot be guaranteed. However, ITS with ITIS reserves the right to deploy proactive technology techniques to detect and suppress wireless networks that interfere with the university wireless network or attempt to simulate LUnet wireless services for malicious purposes.

   b. LUnet wireless services have been designed to allow users in classrooms and gathering areas to access the Internet for limited personal use and to enhance their academic experience. The wireless network is for convenience and has been designed to supplement and enhance the wired network, not replace it. The wireless network as such does not have the capability to provide consistent high quality service for high-bandwidth or latency intolerant applications, such as streaming media, IP telephony, and large file transfers.
5.0 ENFORCEMENT

1. In coordination with administrative departments and law enforcement, SOC and ITIS will investigate any incident involving unauthorized access or improper use of LUnet. User devices or network devices involved in these and other incidents will remain disconnected from LUnet until the user, device owner, or device administrator brings the device into compliance with all relevant policies and standards. ITIS and or SOC will attempt to notify appropriate departmental personnel when disconnecting departmental devices from the network under this provision.

2. SOC or ITIS may require the responsible server administrator to demonstrate compliance with this Policy and the Server Management Policy 10.03.01 through an audit review or other assessment of the offending device and any other devices for which the device administrator is responsible for.

3. Lamar University cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations.

Failure to adhere to the provisions of this policy statement may result in:

1. Loss of Lamar University Information Resources access privileges,

2. Disciplinary action up to and including termination for employees, contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student, or

3. civil or criminal prosecution.

6.0 RELATED DOCUMENTS

1. Lamar University Appropriate Use Policy 10.01.01
2. Lamar University Server Management Policy 10.03.01
3. TAC 202
4. TSUS Government code 2054.003(7) “Information Resources”

7.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every two years

Last Review Date: April 8, 2014

Next Review Date: April 8, 2016
8.0 APPROVAL

Kenneth Evans
President, Lamar University

Priscilla Parsons
Chief Information Officer, Lamar University

April 8, 2014
Date of Approval

April 8, 2014
Date of Approval

9.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Approved Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4/8/2014</td>
<td>Initial Version</td>
</tr>
</tbody>
</table>