# LAMAR UNIVERSITY

## INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology Number: 10.01.09
AREA: Network Management

## SUBJECT: Network Management

### I. PURPOSE

The purpose of this policy is to define a management framework that delineates the roles and responsibilities for the management of all Lamar University networks, network addresses, and network devices. This policy also addresses specific requirements from TSUS rules and regulations regarding network management.

This policy is not intended to cover all the mandated controls by Texas Administrative Code (TAC) 202 and Texas Security Controls Standards (TSCS), but specific requirements from TSUS rules and regulations. Hence network administrators will need to combine requirements from this policy and the Lamar information systems management policy.

### II. SCOPE

This policy applies to all persons and organizations that manage or utilize information technology resources belonging to Lamar University.

### III. DEFINITIONS

See Definition Catalog Version 4 or higher

## IV. ROLES AND RESPONSIBILITIES

*1. Network Management Policy*

1.1. All devices connected to LUnet (regardless of media type) must support Lamar University's mission and initiatives.

1.2. Custodians must develop procedures to facilitate the implementation of the Network Management Policy and associated controls from the Lamar Technical Control Index.

1.3. Custodians must review and update Network Management procedures at a minimum of every *two years.*

2. Authority, Roles, and Responsibilities

2.1. The department of Infrastructure/Operations is designated by the IRM for the management of Lamar University networks with due consideration for accessibility, performance, privacy, compatibility, and security. Part of that operation is the task of protecting network 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.

2.2. Users and custodians of network-connected devices are accountable for device management and network usage practices that might result in damages or harm to network operations, performance, or other network-related devices.

2.3. Users are not permitted to deploy devices or mechanisms that would extend, alter or segment LUnet.

2.4. The department of Infrastructure/Operations is authorized to:

2.4.1. Optimize network flow within the campus network. These optimizations include the prioritization of certain flows or protocols.

2.4.2. Disconnect and confiscate any unauthorized network devices, for example, devices such as home-use routers, access points that would extend, alter, or segment LUnet.

2.5. The office of the Information Security Officer (ISO) is authorized to segment internal network communication. These segmentations include deployment of segmentation-firewalls, traffic shapers, and blocking of certain types of traffic.

2.6. Only the office of the ISO and the department of Infrastructure/Operations are authorized for the interception of network communications. Examples of Network interceptions include scanning, sniffing and packet captures. General purposes for interception include but are not limited to network flow optimization, diagnosis, and incidence response.

2.7. Users are not authorized to intercept network communications without explicit instructions from the office of ISO.

2.8. Users and departments are not authorized to attach or contract vendor services to attach network infrastructure to LUnet without prior authorization from the Department of Infrastructure/Operations.

3. Network address and device management

3.1. The department of Infrastructure/Operations is responsible for:

3.1.1. The planning and coordination for the orderly assignment of all network addresses, including public (internet routable) and private (non-internet routable) addresses.

3.1.2. The planning and coordination of the correct configuration of devices attached to the network.

3.1.3. Designating device administrators for all devices acting in the role of network infrastructure.

3.1.4. Registering all devices acting in the role of network infrastructure in a network registry administered by the office of IRM or designee.

3.1.5. Operating all authoritative resolvers for the "lamar.edu" domain.

3.1.6. Operating all-recursive resolvers for campus networks.

3.2. Campus departments that own and operate domains other than "lamar.edu" and any sub-domains of "lamar.edu" must register the domain and its technical and operational contacts with the office of the IRM.

3.3. The department of Infrastructure/Operations is authorized to deploy proactive technology and techniques to detect and suppress wireless networks that simulate LUnet wireless services for malicious purposes.

3.4. The wireless network is for convenience and has been designed to supplement and enhance the wired network, not replace it.

3.5. The department of Infrastructure/Operations will endeavor to provide a secure wireless network using modern enterprise security standards(wireless) for all users of LUnet wireless networks. Guest Access(wireless) to services on the wireless network may be limited to protocols that incorporate security natively.

3.6. Lamar University does not support devices that do not meet modern enterprise security standards for wireless connectivity.

4. *Threat and Incidence Response*

4.1. Custodians must ensure:

4.1.1. Network devices or addresses that pose an immediate threat to network operations, performance, violate policies or other network-connected devices are disconnected or quarantined to minimize risk until the threat is permanently removed.

4.1.2. Incident response actions comply with established, policy-defined controls and best practices regarding the preservation and treatment of forensic data.

## V. EXCEPTIONS

A. The ISO, with the approval of the Lamar University President, may issue documented exceptions to controls in this policy based on justifications communicated as part of the risk assessment process.

## VI. ENFORCEMENT

A. 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.
3. Dismissal for interns and volunteers.
4. Suspension or expulsion in the case of a student.
5. Civil or criminal prosecution.

## VII. RELATED DOCUMENTS

A. Lamar University Information System Policy
B. Lamar University Technical Control Index
C. Texas Administrative Code (TAC) 202
D. TSUS Rules and Regulation

## VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: 06,02, 2021

Next Review Date: 06,02, 2024

## IX. APPROVAL

President, Lamar University

IRM, Lamar University

### REVISION LOG

| Revision Number | Approved Date | Description of Changes |
|---|---|---|
| **2** | 06,02,2021 | **New Policy** |