LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology Number: 10.01.10
AREA: Server Management

SUBJECT: Server Management

I. PURPOSE

Servers are an essential type of information resource. An information system can be comprised of one or more servers acting as an information resource. Hence servers are utilized to deliver critical components of instruction, research, faculty development, student services and administration in pursuit of the Lamar University mission.

The purpose of this policy is to define a management framework that delineates the roles and responsibilities for the management of all servers, as well as to describe critical roles and responsibilities for server owner and server administrator. This policy also addresses specific requirements from TSUS rules and regulations regarding server management.

This policy is not intended to cover all of the mandated controls by Texas Administrative Code (TAC) 202 and Texas Security Controls Standards (TSCS), but it does include specific requirements from TSUS rules and regulations as well. Hence server owners and server 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. *Server Purpose and Function*
   1.1. Servers may only be provisioned and used for the purpose of supporting university missions.

2. *Server Management Roles and Responsibilities*
   2.1. To effectively mitigate risk and enforce state-mandated security controls, servers that house or process confidential or regulated information must be managed by the IT infrastructure department and must be registered with the office of the IRM, at least biennially. The Senior Director of Infrastructure/Operations is designated as the server owner role for such servers.
   2.2. Servers that do not house or process confidential information that are managed by university departments must be registered with the IRM in a manner specified by the IRM, at least biennially.
   2.3. At a minimum, distinct roles should be delineated for a server owner and a server administrator, and employees assigned to these roles must be registered with the Office of the IRM. If the information system constitutes a single server, then the server owner assumes all responsibilities of the information owner role defined under TAC 202. The server owner is responsible for designating a primary and secondary server administrator. The server administrator assumes all the responsibilities of the information custodian defined under TAC 202.
   2.4. Server owners are responsible for establishing server usage requirements consistent with LU information systems management policy, TAC 202, other university policies, specifying server access controls (both physical and electronic), and assuring compliance with state and the Lamar University Technical Control Index.
   2.5. Server owners are responsible for planning and budgeting fiscal resources required for server maintenance.
   2.6. Administrators are typically responsible for enforcing the owner's usage policies, implementing the owner-specified access controls, and configuring the server according to the Lamar University Technical Control Index.

3. *Server Management Best Practices and Standards*
   3.1. An institutional standard for server management conformance and best practices should be made available to all server owners and administrators by Infrastructure Services. The standard must include controls outlined in the TSUS IT policies, information systems management policies, and the Lamar University Technical Control Index.
   3.2. Compliance review procedures should be established and implemented by server owners. Compliance exceptions should be justified by documented risk management decisions.
   3.3. Ensure that all exceptions granted to this requirement are documented through risk management decisions.

4. *Threat and Incidence Response*
   4.1. Servers that pose an immediate threat to network operations, performance, or other network-connected devices must be disconnected or quarantined to minimize risk until the threat is removed. Incident response procedures and best practices must be followed to ensure appropriate preservation and treatment of forensic data.

V. EXCEPTIONS

A. The Office of 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: 06,01,2024

IX. APPROVAL

_____
President, Lamar University

_____
IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes