1.0 OVERVIEW AND PURPOSE

Servers are utilized to deliver critical components of instruction, research, faculty development, student services, and administration in pursuit of the Lamar University mission. University-wide server management practices that define roles, responsibilities, procedures and controls encourage consistent, secure, and responsible delivery of services.

This policy establishes the framework under which university servers are managed to promote availability, secure information and assets, and mitigate vulnerabilities.

2.0 SCOPE

This policy applies to all university information resources, whether administered remotely, centrally or departmentally, and regardless of where they reside.

Any individual who consumes or utilizes Lamar University information resources agrees to abide by all applicable policies and legal statutes, including all federal, state, and local laws. Lamar University reserves the right at any time to limit, restrict, or deny access to its information resources and to take disciplinary or legal action against anyone in violation of these policies or statutes.

3.0 DEFINITIONS

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 the Lamar University network. 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.

**Public Service** - Any web-facing application designed and delivered with the intent of access by individuals or organizations over the public internet. Public facing applications are exposed to the broadest base of potential users and are accessed via a web-browser.

**Server** – A device that performs a specific service or function on behalf of other network devices or users.

**Server Management** – Functions that enable the server to operate within acceptable parameters of performance, security, availability, and business continuity.

**Server Owner** – The department head charged with overall responsibility for the server asset in the university’s inventory records.

**Server Administrator** – An individual designated by the server owner as principally responsible for performing server management functions, including the installation, configuration, security, monitoring, maintenance, registration, and assessment of the server.

**Security Administrator** – An individual designated by the server owner as principally responsible for performing security management functions, including provisioning, review and monitoring of server accounts.

**ITS** – the Information Technology Division of Lamar University.

### 4.0 POLICY

1. Information resources, including servers, are provided for the purpose of accomplishing tasks related to the university’s mission.

2. Any server that is connected to the university network must comply with this policy, related policies, established standards and procedures.

3. Specific personnel will be identified for each of the following roles:
   a. Server Owner
   b. Server Administrator
   c. Security Administrator

4. Server owners must register their server with the Lamar University Information Technology Services Division and provide yearly verification of all necessary information required in the registration process. Changes to server registration information will be promptly reported to the Information Technology Division.

5. Public services will be disabled for any server that does not meet yearly registration requirements. Server owners and server administrators will participate in and/or conduct a yearly risk assessment of their designated servers based on server registration information.
6. The server owner is responsible for the management, operation, and security of the server. Server administration functions may be designated; however, the server owner retains ultimate responsibility for the server. The server owner will, at a minimum:
   a. Register the server with ITS
   b. Designate a server administrator
   c. Designate a security administrator
   d. Provide fiscal resources required to maintain server policy compliance
   e. Include server management compliance in fiscal planning, business/academic continuity planning, and personnel resource planning.
   f. Ensure proper training for server administrators and security administrators
   g. Respond to any vulnerability scan notifications from ITS
   h. Participate in yearly risk assessments
   i. Ensure that risk mitigation activities identified are resolved within 90 days of risk assessment completion.
   j. With coordination through ITS, respond to audit requests made by TSUS, state or federal audit agencies.

7. Prior to the purchase of any server, the server owner should contact ITS to evaluate the capabilities required to maintain server compliance and review alternative solutions where applicable.

8. ITS will be notified in advance when the purpose, location, management, or disposition of the server changes.

9. ITS will publish server management guidelines for use by server administrators.

10. ITS will conduct routine scans of the university server environment. Vulnerabilities will be communicated to the server owner and server administrator for resolution. The Server owner must respond with an acknowledgement within 3 days. Vulnerabilities that remain unresolved for 30 or more days are subject to disconnect. Servers that pose an immediate threat to network operations, performance, or security may be disconnected or quarantined until the threat is removed.

11. Incident management procedures will be executed by ITS when appropriate.

5.0 ENFORCEMENT

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

10.01.01 Appropriate Use Policy
10.02.03 Data Classification Policy
10.02.02 Security Passphrase Policy

7.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: May 12, 2015

Next Review Date: May 12, 2018

8.0 APPROVAL

Kenneth Evans June 9, 2015
President, Lamar University Date of Approval

Priscilla Parsons June 9, 2015
Chief Information Officer, Lamar University 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>8/6/2012</td>
<td>Initial Version</td>
</tr>
<tr>
<td>2</td>
<td>5/12/2015</td>
<td>Increase the 2 year review cycle to a 3 year review cycle.</td>
</tr>
</tbody>
</table>