LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology Number: 10.01.02
AREA: Information Resources

SUBJECT: System and Service Acquisition Policy

I. PURPOSE

Information technology is a critical enabler in meeting university mission. Information technology resources are strategic and vital assets that belong to people of Texas. These resources must be managed commensurate with their value and in a manner that assures their confidentiality, integrity and availability. Compliance with this policy contributes to the availability, protection, and appropriate use of the information technology resources of Lamar University.

This policy establishes the requirements to assess compliance of products and services which process Lamar University information.

II. SCOPE

This policy applies to all persons and organizations that purchase, develop, manage or utilize information technology resources owned or supplied by or used on behalf of Lamar University, regardless of the source of funds or supplier. Changes to the Finance policy will supersede purchasing related statements in this policy.

III. DEFINITIONS

See Definition Catalog Version 4 or higher

IV. ROLES AND RESPONSIBILITES

A. System and Services Acquisition Responsibilities
   1. The Chief Information Officer (CIO) or designee will be responsible for central review and oversight of all university acquisitions of information technology resources as required by TSUS Rules and Regulations.
   2. Acquisition or use of information technology resources in or through which data is stored and/or exchanged must include an approved and authorized agreement between the university and the provider.
   3. Software License Agreements, Terms of Service, Terms of Use, and written contractual agreements must be signed by duly authorized personnel as per Lamar University Finance procurement policies. University affiliates who individually engage third-party products or services by unauthorized acceptance of Terms of Service or Terms of Use agreements on behalf of Lamar University (online,click-through or otherwise) are personally responsible and liable for any obligations incurred by the agreement, as well as any consequences that result from their engagement with the third-party.
   4. The office of the CIO and the IT Compliance department are responsible to develop and maintain IT acquisition review procedures.
   5. The office of the CIO or the IT Compliance department must facilitate the IT compliance review process.

B. Allocation of Resources
   1. The University planning and budgeting process must include the information security requirements for the information system or service.
   2. The University must determine, document and allocate the resources required to protect information systems or service.
   3. The purchaser must determine, document and allocate the resources required to provide equivalent access through accommodation to information systems or services.

C. System Management Life Cycle
   1. Information security, security testing, and audit controls must be assessed in all phases of the system management lifecycle including during development, acquisition and renewal.
   2. Compliance must be assessed prior to acquisition and upon renewal.

D. Acquisition Process and Procedures
   1. Prior to acquisition, a compliance review shall be completed to assess contractual terms, the need for central IT support, compatibility with information systems and integration, and accessibility of the information resource or service.
   2. No purchase of information resources shall be made prior to completion of the compliance review.
   3. Security capabilities must be provided and reviewed explicitly before the acquisition. The security risk assessment must be in accordance with applicable laws and standards. The documentation required for the evaluation of risk must be in a manner specified by LU IT.
   4. Information systems acquired for university use must be recorded in a registry to facilitate ongoing risk management activities.
   5. The information technology division is authorized to reject acquisitions if incomplete or inaccurate information is provided or the acquisition does not meet compliance and security requirements.

E. Information System Documentation
   1. The information custodian must obtain, protect, and make adequate documentation for the information system available to authorized personnel.

F. Security Engineering Principles
   1. Information systems that house and process confidential information must incorporate security engineering principles in specification, design, development, implementation, and modification of the information system.

G. External Information System Services
   1. Security controls enforced by external service providers must be consistently monitored and reviewed, among which must include controls for authentication and access; audit and

logging; identifier management; authenticator management; communications protection; and integrity protection.

H. Developer Configuration Management
   1. Developers of the information systems or information service must:
      a. Perform configuration management during system, component, or service design, development, implementation and operation.
      b. Document, manage, and control the integrity of changes.
      c. Implement only information owner approved changes to the system, component, or service.
      d. Document approved changes and potential security impacts of such changes.
      e. Track security flaws and flaw resolution.

I. Developer Security Testing and Evaluation
   1. Before implementing an Internet website or mobile application for LU that processes confidential information or sensitive personal or personally identifiable information, the developer must:
      a. Submit a biennial data security plan to the office of the ISO which will be submitted to DIR no later than Feb 15th of each even-numbered year to establish planned beta testing for the website or application; and
      b. Subject the website or application to a vulnerability and penetration test approved by the office of ISO and address any vulnerabilities identified in the test.

J. The Information Security Officer, with the approval of the President, may issue documented exceptions to controls in this policy based on justifications communicated as part of the risk assessment process

V. 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; or
   5. civil or criminal prosecution.

VI. RELATED DOCUMENTS

A. Information Technology Polices and Standards Definition Catalog

VII. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: June 3, 2020

Next Review Date: June 3, 2023

VIII. APPROVAL

Priscilla Parsons
Chief Information Officer

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	6/3/2020	Initial Version