LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology
AREA: Information Technology Area Number: 10.01.02

SUBJECT: System and Service Acquisition Policy

I. PURPOSE

Information technology is a critical component in meeting Lamar University's mission. Information technology resources are strategic and vital assets that belong to the people of Texas. These resources must be managed according to 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 that process Lamar University information and the associated supply chain risks.

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 policies will supersede purchasing-related statements in this policy.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A. SYSTEMS AND SERVICE AQUISITION

1. *Authority and Responsibilities*
   1.1. The Information Resources Manager (IRM) 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 (section19).
   1.2. The Information Technology division is authorized to reject acquisitions if incomplete or inaccurate information is provided, or the acquisition does not meet compliance requirements for security, privacy, compatibility and accessibility.
   1.3. 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 service provider.
   1.4. Software License Agreements, Terms of Service, Terms of Use, and other written contractual agreements must be signed by authorized personnel as per Lamar University Delegation of Authority [MAPP 05.01.06]. Lamar 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 the University (online, click-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.
   1.5. The office of the IRM and the designated department are responsible for developing and maintaining technology acquisition review procedures.
   1.6. The office of the IRM or the designated department must facilitate the technology compliance review process in accordance with applicable regulations.
   1.7. The office of the ISO is responsible for verifying that security requirements are identified, and risk mitigation plans are developed and contractually agreed and obligated prior to the acquisition of new information systems and/or related services and applications.
   1.8. The office of the ISO is responsible for verifying that security requirements are identified, and risk mitigation plans are developed and implemented prior to the deployment of internally developed information systems and/or related applications or services.

2. *Allocation of Resources [SA-2]*
   2.1. Lamar University must:
      2.1.1. Determine high-level information security requirements for each information system or information system service in mission and business process planning.
      2.1.2. Determine, document, and allocate the resources required to protect each information system or information system service as part of its capital planning and investment control process.
      2.1.3. Establish a discrete line-item for information security in institutional programming and budgeting documentation.

3. *System Development Life Cycle (SDLC) [SA-3]*
   3.1. Owners and custodians must:
      3.1.1. Acquire, develop, and manage the information system that incorporates information security and privacy considerations using an SDLC.
      3.1.2. Define and document information security and privacy roles and responsibilities throughout the SDLC.
      3.1.3. Identify individuals that have information security and privacy roles and responsibilities.
      3.1.4. Integrate Lamar University's information security and privacy risk management processes into SDLC activities.

3.1.5. Include information security, security testing, and audit controls in all phases of the system development lifecycle or acquisition process.

4. *Acquisition Process [SA-4]*
   4.1. Prior to acquisition:
      4.1.1. A compliance review must be completed to assess contractual terms, privacy terms, technology dependencies including the need for central IT support, compatibility with information systems and integration, and accessibility of the information resources or services.
      4.1.2. Security capabilities must be provided and reviewed explicitly.
      4.1.3. The security risk assessment must be in accordance with applicable laws and standards.
      4.1.4. The information system owner must facilitate the documentation required for the evaluation of risk must be in a manner specified by Lamar University's IT Division.
      4.1.5. The following requirements must include descriptions, and criteria, explicitly or by reference, in the acquisition contract for each information system, information system component, or information system service, in accordance with applicable federal/state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
         4.1.5.1. Security functional requirements.
         4.1.5.2. Strength of mechanism requirements.
         4.1.5.3. Security assurance requirements.
         4.1.5.4. Controls to satisfy security requirements.
         4.1.5.5. Security-related documentation requirements.
         4.1.5.6. Requirements for protecting security-related documentation.
         4.1.5.7. Description of the information system development environment and environment in which the system is intended to operate.
         4.1.5.8. Allocation of responsibility or identification of parties responsible for information security and supply chain risk management.
         4.1.5.9. Acceptance criteria.
      4.1.6. When entering or renewing a contract with a vendor authorized to access, transmit, use or store confidential or regulated data, Lamar University must include within, or as an addendum to the contract, the "Information Security and Accessibility Standards Exhibit", from the TSUS Contract Management Handbook, or if superseded, the appropriate addendum replacing the exhibit.
   4.2. Prior to contracting or renewing cloud computing services that store, or process confidential or regulated data, Lamar University must:
      4.2.1. Ensure that vendors are certified through TX-RAMP (Texas Risk and Authorization Management Program), on or after January 1, 2022.
      4.2.2. Require vendors that are subject to TX-Ramp, to maintain program compliance and certification throughout the term of the contract.

5. *Information System Documentation [SA-5]*
   5.1. Owners and Custodians must:
      5.1.1. Obtain administrator documentation for each information system, information system component, or information system service that describes:
         5.1.1.1. Secure configuration, installation, and operation of the system, component, or service.
         5.1.1.2. Effective use and maintenance of security functions/mechanisms.
         5.1.1.3. Known vulnerabilities regarding configuration and use of administrative or privileged functions.
      5.1.2. Obtain user documentation for each information system, information system component, or information system service that describes:
         5.1.2.1. User-accessible security functions and mechanisms and how to effectively use those security functions/mechanisms**.**

5.1.2.2. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.

5.1.2.3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.

5.1.3. Document attempts to obtain information system, information system component, or information system service documentation. When such documentation is either unavailable or nonexistent recreate the documentation if it is essential to the implementation and operation of the system.

5.1.4. Protect documentation as required, in accordance with the organizational risk management strategy.

5.1.5. Distribute documentation to relevant personnel or roles.

6. *Security Engineering Principles [SA-8]*

6.1. Apply the security engineering principles as defined in the LTCI, in specification, design, development, implementation, and modification of the information system and information system components.

7. *External System Services [SA-9]*

7.1. Lamar University must:

7.1.1. Require that providers of external information system services comply with university information security requirements and employ university defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

7.2. Owners and custodians must:

7.2.1. Define and document university oversight and user roles and responsibilities with regards to external information system services.

7.2.2. Employ university defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

8. *Developer Configuration Management [SA-10]*

8.1. Lamar University must require the developer of each information system, information system component, or information system service to:

8.1.1. Perform configuration management during at least one of the following life cycle stages: design, development, implementation, operation, or disposal.

8.1.2. Document, manage, and control the integrity of changes to university defined configuration items under configuration management.

8.1.3. Implement only university approved changes to the information system, information system component, or information system service.

8.1.4. Document approved changes to the information system, information component, or information system service and the potential security impacts of such changes.

8.1.5. Track security flaws and flaw resolution within the information system, information system component, or information system service and report findings to custodians and the office of the ISO.

8.2. The information owner approves all security-related information resources changes for their respective information system(s) through a change control process.

8.3. The approval of such changes to occur prior to the implementation of the security-related information resources changes by the University or independent contractors.

9. *Developer Security Testing and Evaluation [SA-11]*

9.1. Lamar University must require the developer of the information system, information system component, or information system service, at all post-design stages of the system development life cycle, to:

9.1.1. Develop and implement a plan for ongoing security assessments.

9.1.2. Perform the appropriate level and frequency of testing and evaluation based on the classification of data and the security categorization of the information system.
9.1.3. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation.
9.1.4. Implement a verifiable flaw remediation process.
9.1.5. Correct flaws identified during testing and evaluation.

10. Unsupported Systems Component [SA-22]
10.1. Lamar University must:
10.1.1. Replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer.
10.1.2. Provide alternative sources for continued support for unsupported components (e.g., support from external providers, in-house support if technically feasible).

B. SUPPLY CHAIN RISK MANAGEMENT

1. *Supply Chain Risk Management Plan [SR-2]*
1.1. Lamar University must:
1.1.1. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of organization-defined information systems, system components or system services.
1.1.2. Implement the supply chain risk management plan consistently across the university.
1.1.3. Review and update the supply chain risk management plan at least every 5yrs, to address threat, organizational or environmental changes.

2. *Supply Chain Controls and Processes [SR-3]*
2.1. Lamar University must:
2.1.1. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of organization-defined information systems or information system components in coordination with organization-defined personnel or roles.
2.1.2. Employ organization-defined supply chain controls to protect against supply chain risks to information systems, information system components, or information system services and to limit the harm or consequences of supply chain-related events.
2.1.3. Document the selected and implemented supply chain processes and controls in a security plan.

3. *Acquisition Strategies, Tools and Methods [SR-5]*
3.1. Lamar University must:
3.1.1. Employ organization-defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

4. *Notification Agreements [SR-8]*
4.1. Lamar University must:
4.1.1. Establish agreements and procedures with entities involved in the supply chain for information systems, information system components, or information system services for the one or more of the following:
4.1.1.1. Notification of supply chain compromises.
4.1.1.2. Results of assessments or audits.

4.1.1.3. Organization-defined information and controls.

5. *Component Disposal [SR-12]*
   5.1. Lamar University must:
      5.1.1. Dispose of confidential and regulated data, documentation, tools, and/or information system components using organization-defined techniques and methods.

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. Information Technology Policies and Standards Definition Catalog.
B. Information Systems Management Policy.
C. The Texas State University System Rules and Regulations (Section 19).
D. Lamar University Manual of Administrative Policies and Procedures. (MAPP 05.01.06).

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: IRM

Review Schedule: Every three years

Last Review Date: 07/07/2025

Next Review Date: 07/07/2028

IX. APPROVAL

Jaime Taylor – 09/25/2025

_____

President, Lamar University

Patrick Stewart – 09/25/2025

_____

IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
2	**07/14/2025**	**Signed authorized personnel amended from Lamar University Finance Procurement Policies to Delegation of Authority MAPP 05.01.06.** **Authority and Responsibility – New policy statements.** **SA[3] – New policy statement.** **SA[4] – New policy statement.** **SA[5] – New policy statement.** **SA11 – New policy statement.** **SA[9] – New policy statement.** **SA[10] – New policy statement.** **SA[11] – New policy statement.** **SA[22] – New policy statement.** **SR Family – New Family.**