POLICY LIT.3.06
USE OF CLOUD SERVICES

SCOPE: Faculty, Staff, and Students

1. POLICY STATEMENT

This policy establishes a framework for the use of Cloud Services to ensure that Lamar Institute of Technology (LIT) data is appropriately stored, processed, shared, and managed on those services.

2. DEFINITIONS

2.1. A listing of initialisms used in this and other information resources policies can be found in Appendix A.

2.2. A glossary with definitions of terms used in this and other information resources policies can be found in Appendix B.

3. APPLICABILITY

3.1. This policy applies to LIT faculty, staff, contractors, vendors, and anyone else doing business with the college who has access to college data.

3.2. This policy applies to all types of Cloud Services that are utilized to store, process, share, transmit, or manage college data.

3.3. Information that is used solely for classroom instruction purposes (e.g., lecture notes or PowerPoint slides for teaching) and is not classified as Confidential or Sensitive (see Policy LIT.3.04 Information Security Program, Section 5) is exempt from this policy.

4. GENERAL INFORMATION

4.1. The use of Cloud Services must comply with applicable TSUS Rules and Regulations, Lamar Institute of Technology Policies, and federal and state laws and regulations. Any decision to use Cloud Services should consider the risks and liabilities related to security, privacy, retention, access, and compliance.

4.2. Storage, processing, sharing, transmitting, and managing of Confidential, Sensitive or Mission Critical data is only allowed on approved and contracted Cloud Services.

4.3. Cloud Services must not be engaged without:

4.3.1. developing an exit strategy for disengaging from the vendor or service;

4.3.2. integrating the service into business continuity and disaster recovery plans; and

4.3.3. determining how data would be recovered.

4.4. Cloud Services are covered by the same acceptable use and information security policies that govern all other computing resources.

4.5. Institute data stored using a Cloud Service are college records and appropriate records retention requirements must be followed.

5. CLOUD COMPUTING SERVICE PROVIDERS ELIGIBILITY / APPROVAL

5.1. Cloud Service Providers must be approved by the IRM and ISO. Providers shall be selected based on data classification and risk.

5.2. The IRM shall maintain a list of approved Cloud Service Providers.

5.3. Use of Cloud Services involves delegating custody and aspects of data security to the Cloud Service Provider. Cloud Service Providers that will be used to store, process, share, transmit, or manage college data classified as Confidential, Sensitive, or Mission Critical must be contractually obligated with LIT to assume the appropriate delegated responsibilities.

5.4. LIT provides employees with cloud-based services such as Office 365, OneDrive, and Microsoft Teams, which can be accessed from both on campus and off campus computing devices. Faculty and staff are expected to consider Institute-provided Cloud Services before procuring alternative Cloud Services.

6. PERSONAL CLOUD COMPUTING SERVICES

6.1. Personal Cloud Services (services for which the agreement is with an individual and not LIT) may not be used to store, process, share, transmit, or manage college data classified as Confidential, Sensitive, or Mission Critical. This includes educational records subject to FERPA.

7. EXCEPTIONS

Exceptions to this policy may be granted under certain circumstances. Requests for exceptions should be sent to the IRM.

Related Procedures:

Relevant Forms/Documents:

Relevant TSUS Policies/Forms/Documents:

Relevant Statutes:

Relevant SACSCOC Standards:

Document History:
Adopted:
Reviewed:
Revised: September 2025