LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology
AREA: Risk Management Area Number: 10.01.05

SUBJECT: Risk Management Policy

I. PURPOSE

The management of organizational risk is a critical element of the University's information security program and provides an effective framework for selecting the appropriate security controls for an information system. Security controls are necessary to protect individuals and the operations and assets of the University.

The purpose of the risk management policy is to facilitate processes that integrate security and risk management activities into the information system management life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.

In the risk-based approach to information system management, the selection and specification of security controls for an information system are accomplished as part of the system security plan. The selected controls are implemented, assessed, and the information system is authorized for operation. The information system is then continuously monitored for the effectiveness of implemented controls.

This policy addresses requirements from three families of controls specified in the Texas Control Standards Catalog (TCSC) and Texas Administrative Code (TAC) 202 to adopt a risk-based information system management framework.

In the context of this policy, the term information system custodian is used in place of Texas state defined custodian for clarity and to avoid conflict where applicable.

II. SCOPE

This policy applies to Lamar University affiliates. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their management and use of the University's information resources.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A. PLANNING

1. *System Security Plan [PL-2]*
   1.1. The Office of the Information Security Officer (ISO) must:
      1.1.1. Develop a security plan for the information system that, at minimum.
         1.1.1.1. Is consistent with the University's enterprise architecture.
         1.1.1.2. Explicitly defines the authorization boundary for the system.
         1.1.1.3. Describes the function and security posture of the information system in terms of missions and business processes.
         1.1.1.4. Provides the security categorization of the information system, including supporting rationale.
         1.1.1.5. Describes the operational environment for the information system and relationships with or connections to other information systems.
         1.1.1.6. Provides an overview of the security requirements for the system.
         1.1.1.7. Identifies any relevant overlays, if applicable.
         1.1.1.8. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions.
         1.1.1.9. Is reviewed and approved by the information owner or designated representative prior to the planned implementation.
      1.1.2. Distributes copies of the security plan and communicates subsequent changes to the plan to owners and custodians.
      1.1.3. Reviews the security plan for the information system prior to periodic risk assessment.
      1.1.4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
      1.1.5. Protects the security plan from unauthorized disclosure and modification.

2. *Rules of Behavior [PL-4*]
   2.1. Lamar university must:
      2.1.1. Establish the rules that describe user responsibilities and expected rules of behavior with regard to information and information system usage.
      2.1.2. Make the rules available to individuals requiring access to the information system.
      2.1.3. Receive a signed acknowledgment from individuals, indicating that they have read, understood, and agreed to abide by the rules of behavior before authorizing access to information and the information system.
      2.1.4. Review and update rules of behavior every 5years.
      2.1.5. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

B. SECURITY ASSESSMENT AND AUTHORIZATION

1. *Security Assessment [CA-2]*
   1.1. Lamar university must:
      1.1.1. Develop a security assessment plan that describes the scope of the assessment, including:
         1.1.1.1. Security controls and control enhancements under assessment
         1.1.1.2. Assessment procedures to be used to determine security control effectiveness.
         1.1.1.3. Assessment environment, assessment team, and assessment roles and responsibilities.
      1.1.2. In accordance with TGC2054 515.a, assess the security controls in the information system and its environment of operation, at least once every two

years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

1.1.3. Produce a security assessment report that documents the results of the assessment.

1.1.4. In accordance with TGC2054 515.b, provide the results of the security control assessment not later than December 1, of the year in which the University conducts the assessment to.

1.1.4.1. DIR

1.1.4.2. The governor, the lieutenant governor, and the speaker of the house of representatives, on their request.

1.1.4.3. The Office of the ISO, information owner, custodian, IRM, and the President.

2. *System Interconnections [CA-3]*

2.1. Lamar university must:

2.1.1. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

2.1.2. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated in:

2.1.2.1. The Security plan for systems managed by the University that have the same authorizing officials.

2.1.2.2. A formal Contracts between Lamar and external entities for systems between organizations

2.1.3. Review and update Interconnection Security Agreements, as necessary.

3. *Plan of Action and Milestones [CA-5]*

3.1. Information system custodians must:

3.1.1. Develop a plan of action and milestones for an information system to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

3.1.2. Update the existing plan of action and milestones as required, based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

4. *Security Authorization [CA-6]*

4.1. Lamar university must:

4.1.1. Assign a senior executive as the Authorizing Official for each information system.

4.1.2. Ensure that the Authorizing Official for an information system authorizes the information system for processing before commencing operations.

4.1.3. Update the security authorization at the time of periodic risk assessment for the information system or biennially.

5. *Continuous Monitoring [CA-7]*

5.1. Lamar University must develop continuous monitoring and implement a continuous monitoring program that includes:

5.1.1. Establishment of metrics to be monitored.

5.1.2. Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring.

5.1.3. Ongoing security control assessments in accordance with the institutional continuous monitoring strategy.

5.1.4. Ongoing security status monitoring of institution-defined metrics in accordance with the institutional continuous monitoring strategy.

5.1.5. Correlation and analysis of security-related information generated by assessments and monitoring.

5.1.6. Response actions to address results of the analysis of security-related information.

5.1.7. Reporting the security status of the institution and the information system to appropriate stakeholders at least every two years.

6. *Penetration Testing [CA-8]*

6.1. The Office of the ISO is responsible for coordinating penetration testing of internet websites or mobile applications that process SPI, PII, or confidential information at a frequency as deemed necessary by the ISO, in accordance with Texas Government Code (TGC) 2054.516.2.

7. *Internal System Connection [CA-9]*

7.1. Information system custodians must:

7.1.1. Review and authorize internal connections of classes of components to the information systems that house or process confidential information. Examples of classes of components include printers, copiers, fax machines, scanners and sensors, and servers.

7.1.2. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

C. RISK ASSESSMENT

1. Security Categorization [RA-2]

1.1. The Office of the ISO must establish requirements for the security categorization of information systems.

1.2. In accordance with TAC 202.72.1.a, the owner must:

1.2.1. Categorize information and the information system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations and standards.

1.2.2. Document the security categorization results (including supporting rationale) in the security plan for the information system.

1.2.3. Ensure that the Office of the ISO reviews and approves the security categorization decided by the Information owner.

2. Risk Assessment [RA-3]

2.1. The owner and information system custodian must:

2.1.1. Participate in the risk assessment conducted by the Office of the ISO to assess the likelihood and magnitude of the harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

2.1.2. Document risk assessment results in a manner specified by the Office of the ISO.

2.2. The owner must review the results of the risk assessment at the following frequencies or whenever there are significant changes to the information system, environment of operation or other conditions that may impact the security state of the system:

2.2.1. At least annually for information systems with high residual risk.

2.2.2. At least bi-annually for information systems with moderate residual risk.

2.2.3. At least every three years for information systems with low residual risk.

2.3. Authorization of security risk acceptance, transference, or mitigation decisions shall be the responsibility of:

2.3.1. The ISO or their designee(s), in coordination with the information owner, for systems identified with low or moderate residual risk.

2.3.2. The University President for all systems identified with a high residual risk.

3. Vulnerability Scanning [RA-5]

3.1. The Office of the ISO must:

3.1.1. On a bi-monthly basis, scan for, and remediate, vulnerabilities in the

information system and hosted applications before commencing operations, and when new vulnerabilities potentially affecting the system/applications are identified and reported.

3.1.2. Employ automatically updated vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
3.1.2.1. Enumerating platforms, software flaws, and improper configurations
3.1.2.2. Formatting checklists and test procedures.
3.1.2.3. Measuring vulnerability impact.

3.1.3. Notify custodians of corrective actions when sensitive information about the information system is discoverable publicly. Typically, discoverable information is information that can be obtained without directly compromising or breaching the information system.

3.1.4. Analyze vulnerability scan reports and results from security control assessments.

3.1.5. Share information obtained from the vulnerability scanning process and security control assessments with custodians' other entities to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)

3.2. The Office of the ISO is authorized to conduct authenticated, privileged scans on information system components even if such scans may be deemed intrusive.

3.3. Information system custodians are responsible for remediating legitimate vulnerabilities within 30 calendar days in accordance with the University's assessment of risk.

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. Texas Control Standards catalog.

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: 2021-07-06

Next Review Date: 2023-06-09

IX. APPROVAL

_____
President, Lamar University

_____
IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	2021-06-09	New policy