POLICY LIT.3.04
INFORMATION SECURITY PROGRAM

SCOPE: Faculty, Staff, Students, and Guests

1. POLICY STATEMENT

1.1. 1 Tex. Admin. Code §202 requires each institution of higher education to develop, document, and implement an institution-wide information security program, approved by the institution head or delegate, that includes protections, based on risk, for all information and information resources owned, leased, or under the custodianship of an department, operating unit, or employee of the institution of higher education including outsourced resources to another institution of higher education, contractor, or other source. In compliance with 1 Tex. Admin. Code §202, this policy statement and its references reflect the policies, procedures, standards, and guidelines comprising Lamar Institute of Technology's (LIT) information security program.

1.2. Information that is Sensitive or Confidential must be protected from unauthorized access or modification. Data that is essential to critical university functions must be protected from loss, contamination, or destruction.

1.3. Information must be identified and assigned the appropriate data classification in order to be protected appropriately.

1.4. Appropriate roles and responsibilities must be identified to facilitate data protection.

1.5. This policy articulates a framework for LIT's information security program.

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. ROLES AND RESPONSIBILITIES

3.1. *All members of the LIT community* share responsibility for protecting LIT's information resources and, as such, are essential components of LIT's information security organization. Although some roles are reserved for certain positions within the Institute, each individual may assume one or more roles with respect to each information resource they use, and as a result, are accountable for the responsibilities

attendant to their roles. Responsibilities associated with each role are noted throughout this and other LIT information resources policies.

3.2. President

3.2.1. The President may delegate some or all the operational duties in Section 3.2.2 of this policy; however, the President remains ultimately responsible for the security of Institute information resources.

3.2.2. The President or designated representative must:

3.2.2.1. Designate an Information Security Officer (ISO). The ISO must possess the training and experience required to perform the duties required by 1 Tex. Admin. Code §202, must report to executive management and must have the explicit authority and duty to administer the information security requirements of this policy college wide.

3.2.2.2. Allocate sufficient resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to an acceptable level to the President.

3.2.2.3. Ensure senior management and information resource owners, in collaboration with the Information Resources Manager (IRM) and ISO, support the provision of information security for the information systems that support the operation and assets under their direct or indirect control.

3.2.2.4. Ensure that the college has trained personnel to assist in complying with the requirements of the Institute's information security and related policies.

3.2.2.5. Ensure senior management support the ISO in developing required security reporting as described in Section 8 of this policy.

3.2.2.6. Approve any risk management decisions for information systems with residual risk assigned a ranking of High identified through risk assessment.

3.2.2.7. Annually, review and approve the college's information security program.

3.2.2.8. Ensure that information security management processes are part of LIT's strategic planning and operational processes.

3.2.2.9. Approve exceptions to information security requirements or controls as per the exception process described in Section 6 of this policy.

3.3. Information Security Officer (ISO)

3.3.1. The ISO must:

3.3.1.1. Develop and maintain a college-wide information security plan, in accordance with Texas Government Code §2054.133.

3.3.1.2. Develop and maintain information security policies and procedures that address the requirements of 1 Tex. Admin. Code §202 and LIT's information security risks.

3.3.1.3. Work with the college's business and technical resources to ensure that controls are utilized to address all applicable security requirements and the college's information security risks.

3.3.1.4. Provide for training and direction of personnel with significant responsibilities for information security with respect to those responsibilities.

3.3.1.5. Administer an ongoing information security awareness education program.

3.3.1.6. Provide guidance and assistance to senior LIT officials, information owners, information custodians, and users concerning their responsibilities under 1 Tex. Admin. Code §202.

3.3.1.7. Ensure risk assessments are performed by the information owners and supported by the information custodians at least biennially for systems containing confidential data and periodically for systems containing institution of higher education sensitive or public data.

3.3.1.8. Ensure information security assessments are conducted biennially for systems containing confidential data and periodically for systems containing sensitive or public data.

3.3.1.9. Review LIT's inventory of information systems and related ownership and responsibilities.

3.3.1.10. 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.

3.3.1.11. 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.

3.3.1.12. Coordinate the review of the data security requirements specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data.

3.3.1.13. Report, at least annually, to the President and executive management of the college the status and effectiveness of the security program and its controls.

3.3.1.14. Inform any relevant parties in the event of noncompliance with the college's information security and related policies.

3.3.1.15. Approve, in coordination with the information owner, risk management decisions for information systems with residual risk assigned a ranking of Low or Moderate identified through risk assessment.

3.3.1.16. Implement a threat awareness program that includes a cross-organization information-sharing capability.

3.4. Information Resources Manager (IRM)

3.4.1. The IRM is the designated default Authorizing Official for all LIT information systems.

3.5. Information Owners

3.5.1. LIT (and consequently the state of Texas) is the legal owner of all the information assets of the college. Ownership of data, information, and records (all hereinafter referred to as information) maintained in the manual and automated information and records systems of LIT is identified in Table 1.

Table 1: Information Owners

Information Type	**Information Owner**
Employment Records	Executive Director for Human Resources
Current and Former Student Information	Registrar
Financial Information	Vice President for Finance and Operations/ Chief Financial Officer
Donor Information	President
Prospective Student Information	Registrar
Student Financial Aid Information	Director of Financial Aid
Information Security	Chief Information Security Officer
Unit Administrative Information	Unit Head
Other	President

3.5.2. Ownership responsibility for on-premises network and system infrastructure hardware is assigned to the IRM by default.

3.5.3. Information owners must:

3.5.3.1. Classify information under their authority, with the concurrence of the IRM and ISO, in accordance with this policy.

3.5.3.2. Approve access to information resources and periodically review access lists based on documented risk management decisions.

3.5.3.3. Formally assign custody and authorize the custodian(s) to implement required security controls.

3.5.3.4. Coordinate data security control requirements with the ISO and convey said requirements to information custodians.

3.5.3.5. Justify, document, and accept accountability for exceptions to security controls issued by the ISO for the information for which the Information Owner is responsible.

3.5.3.6. Coordinating and obtaining approval for exceptions to security controls as per the process described in Section 7 of this policy.

3.5.3.7. Complete risk assessments as described in Policy LIT.3.05 Information Security Control Standards, Section 17.

3.5.3.8. Coordinate with the ISO on the approval of risk management decisions for information systems with residual risk assigned a ranking of Low or Moderate identified through risk assessment.

3.6. Information Custodians

3.6.1. Multiple entities may be designated as information custodians. LIT Information Technology Services department is, by default, a custodian of all information resources for which it has system administration responsibilities. Third party entities providing outsourced information resources services to the institution may be designated as information custodians, as appropriate.

3.6.2. Information custodians must:

3.6.2.1. Participate in risk assessments as described in Policy LIT.3.05 Information Security Control Standards, Section 17.

3.6.2.2. Provide information necessary to support appropriate employee information security training.

3.6.2.3. In consultation with the IRM and ISO where possible and practical, information custodians must:

3.6.2.4. Implement required security controls based on the classification and risks specified by the owner or as specified by LIT's policies, procedures, and standards.

3.6.2.5. Provide owners with information to evaluate the cost-effectiveness of controls and monitoring.

3.6.2.6. Adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents.

3.6.2.7. Supply any information and/or documents necessary to provide appropriate information security training to employees.

3.6.2.8. Ensure information is recoverable in accordance with risk management decisions

3.7. Users

3.7.1. Users of information resources must use them only for the purpose specified by the institution or the information owner.

3.7.2. Users must comply with LIT policies, procedures, security bulletins, and alerts issued by LIT Information Technology Services or the ISO to prevent unauthorized or accidental disclosure, modification, or destruction of information.

3.7.3. Users must formally acknowledge that they will comply with LIT information security policies and procedures in a method determined by the college.

3.7.4. Employee users are responsible for ensuring the privacy and security of the information they access in the normal course of their work. They are also responsible for the security of any computing equipment used in the normal course of work.

4. GENERAL

4.1. The college must develop, document, and implement a college-wide information security program.

4.2. The ISO will lead the development of the program.

4.2.1. All units with operational responsibility for various aspects of information security (e.g., physical security, personnel security, technical security controls) must contribute to program creation, maintenance, and implementation.

4.2.2. The program must include:

4.2.2.1. Risk-based protections for all information and information resources owned by, leased by, or under the custodianship of LIT, including outsourced resources to another institution of higher education, contractor, or other source (e.g., cloud computing).

4.2.2.2. Periodic assessments (in alignment with minimum legal reporting requirements) of the risk and impact that could result from the

unauthorized access, use, disclosure, disruption, modification, or destruction of information, information systems, and applications that support Institute operations and assets.

4.2.2.3. Policies, controls, standards, and procedures that:

4.2.2.3.1. Are based on risk assessments.

4.2.2.3.2. Cost-effectively reduce information security risks to a level acceptable to the President.

4.2.2.3.3. Ensure that information security is addressed throughout the life cycle of each LIT information resource.

4.2.2.3.4. Ensure compliance with relevant federal and state legislative requirements (e.g., 1 Tex. Admin. Code §202), Texas State University System policies, LIT information security policies, and minimally acceptable system configuration requirements as determined by LIT.

4.2.2.4. Strategies to address risk to information resources assigned an impact ranking of High through risk assessment.

4.2.2.5. Risk-based plans for providing information security for networks, facilities, and systems or groups of information systems and applications.

4.2.2.6. A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in LIT information security policies, procedures, and practices.

4.2.3. A process to justify, grant and document any exceptions to specific program requirements in accordance with Section 7 of this policy.

4.3. The program and associated plans and procedures must be reviewed and updated on an annual basis. Additional review and updates must be triggered by any changes that impact information security, security risk assessments, and implementation issues.

4.4. Program, plan, and procedure documentation, including security-related plans identified in this and other LIT information resources policies is confidential under Texas Government Code §552.139 and must be protected from unauthorized disclosure or modification.

5. DATA CLASSIFICATION

5.1. All information stored, processed, or transmitted using LIT's information systems must be identified and assigned the appropriate classification of Public, Sensitive, or Confidential.

5.2. Information that meets the criteria for Mission Critical must be assigned that classification in addition to the primary classification.

5.3. Sensitive or Confidential information must be protected from unauthorized access or modification.

5.4. Mission Critical information must be protected from loss, misuse, unauthorized disclosure or access, unauthorized modification, or unauthorized destruction, as applicable.

5.5. Assigned classifications must be included in an information asset inventory maintained by LIT's Information Technology Services department.

5.6. All information must be reviewed and classified prior to being posted on a publicly accessible information system (e.g., public website) to ensure nonpublic information is not included.

6. INFORMATION SECURITY RISK MANAGEMENT

6.1. Risk assessments for information and information systems must be completed as per Policy LIT.3.05 Information Security Control Standards, Section 13.

6.2. The ISO and owners must identify remedial actions to correct weaknesses or deficiencies noted during the risk assessment process. These actions must be documented in a plan of action and milestones, to be updated based on findings from subsequent risk assessments, security impact analyses, and monitoring activities.

6.3. The ISO will commission periodic reviews of LIT's information security program. Reviews will be conducted at least biennially by individuals independent of the information security program and will be based on business risk management decisions.

7. INFORMATION SECURITY EXCEPTIONS

7.1. Exceptions to security requirements or controls may be granted to address circumstances or business needs. They must be justified and documented.

7.2. Requests for exceptions must be initiated by the information resource owner (as the accountable party) and submitted to the ISO.

7.3. Requests must contain the following information:

7.3.1. The policy for which the exception is sought.

7.3.2. The information resources and the data included in the exception.

7.3.3. The reason for the exception (e.g., why compliance with the policy is not feasible).

7.3.4. Workarounds, compensating security controls, or other mitigation activities in place.

7.3.5. Risk management rationale.

7.4. Each request will be reviewed by the ISO and IRM. After any questions or concerns are addressed, the ISO will accept or reject the exception with the concurrence of the IRM. Exceptions for which there is high residual risk, require the approval of the LIT President.

7.5. Approval may be contingent upon the application of compensating security controls to reduce risk resulting from the exception. All approvals will have an expiration date no longer than two (2) years from the request date.

7.6. A record of all requests and their disposition must be maintained by the ISO.

7.7. Approved security exceptions must be included in LIT's risk assessment process.

8. INFORMATION SECURITY REPORTING

8.1. The ISO will report to the LIT President and executive management at least annually on the following topics:

8.1.1. The adequacy and effectiveness of LIT's information security policies, procedures, and practices, as determined by risk assessment.

8.1.2. Compliance with information security requirements.

8.1.3. Residual risks identified by the Institute's risk management process.

8.1.4. The effectiveness of the current information security program and the status of key initiatives.

8.1.5. The Institute's information security requirements and requests such as security exceptions and requests for resources.

8.2. The ISO will complete the Biennial Information Security Plan, in accordance with Texas Government Code §2054.133.

8.3. The ISO will complete and submit an information security assessment in compliance with the requirements of Texas Government Code §2054.515 and 1 Tex. Admin. Code §202.73(c)

8.4. The ISO will comply with the following Texas State University System (TSUS) reporting requirements:

8.4.1. Notification to System Administration via the Vice Chancellor and Chief Financial Officer and the Chief Audit Executive of any Urgent Incident Reports made to the Texas Department of Information Resources. (See Policy LIT.3.05 Information Security Control Standards, Section 10.)

Related Procedures:

Relevant Forms/Documents:

Relevant TSUS Policies/Forms/Documents: Policy LIT.3.01 Information Resources Management; Policy LIT.3.05 Information Security Control Standards

Relevant Statutes: 1 Tex. Admin. Code §202.70; 1 Tex. Admin. Code §202.71; 1 Tex. Admin. Code §202.72; 1 Tex. Admin. Code §202.73; 1 Tex. Admin. Code §202.74; 1 Tex. Admin. Code §202.75; Texas Government Code §2054.133; Texas Government Code § 552.139

Relevant SACSCOC Standards:

Document History:
Adopted:
Reviewed:
Revised: September 2025