LAMAR UNIVERSITY
MEMBER THE TEXAS STATE UNIVERSITY SYSTEM™

DOCUMENT NAME INFORMATION SECURITY PROGRAM
EFFECTIVE DATE July 6, 2021

Executive Summary

An Information Security Program (ISP) is designed to protect information and critical resources from a wide range of threats, to ensure business continuity and minimize business risk. Information resource security is achieved by implementing applicable policies, processes, procedures, controls, standards, guidelines, organizational structures and supporting technology. These components, where necessary, must be established, implemented, monitored, reviewed, and improved to ensure that the specific security and business objectives of Lamar University are met.

The ISP governs the confidentiality, integrity, and availability of Lamar University data, especially highly sensitive or critical data, and defines the roles and responsibilities of departments and individuals for such data.

Information resource management is governed by several federal and state laws, administrative codes, and Texas State University System (TSUS) rules and regulations. In particular, Texas Administrative Code (TAC) 202 subchapter C and Texas Government Code 2024(TGC) defines information security standards for institutions of higher education. The rules in TAC & TGC define the requirements of the information security program, responsibilities of the President, Information Resources Manager (IRM), Information Security Officer (ISO), staff and users of information resources. Additionally, TAC also mandates the university-wide adoption of appropriate security controls, which are reported to the Texas Department of Information Resources (DIR), biennially.

This document establishes Lamar University's information security program (ISP) as mandated by Texas Administrative Code (TAC), Texas Government Code (TGC) and Texas State University System (TSUS) rules and regulations. The information security program establishes the components of Lamar University information security management and outlines Lamar University's objectives for managing, operating and controlling information security activities.

Table of Contents

Introduction

This document establishes Lamar University's Information Security Program (ISP) as mandated by Texas Administrative Code (TAC), Texas Government Code (TGC) and Texas State University System (TSUS) rules and regulations. The ISP establishes the components of Lamar University information security management and outlines Lamar University's objectives for managing, operating and controlling information security activities.

Where applicable, policies, procedures, standards, guidelines and controls are established to support and maintain the information security program.

Policies serve as overarching rules for the use, management, and implementation of information security throughout Lamar University.

Procedures, standards, and guidelines serve to define the methods for the protection of information assets and preserve the privacy of users, using hardware and software functions.

Defined controls provide a system of checks and balances intended to identify irregularities, reduce risks, prevent abuse, and assist in resolving discrepancies that are introduced in the operations of the business.

Purpose

The purpose of the information security program is to:

- Ensure the confidentiality, integrity, and availability of university data.
- Satisfy and maintain compliance with applicable laws, codes, controls, rules and regulations.
- Reflect Lamar University's commitment to stewardship of sensitive and critical business information.
- Establish the governance and responsibilities for information security at the university.
- Establish a requirement for periodic assessments of risk and impact resulting from unauthorized access, use, disruption or destruction of information and information systems that support Lamar University.
- Provide for information classification and establish controls for each classification type.
- Establish an ongoing security awareness education program for all users starting with new employees during onboarding process.
- Establish strategies to protect high-impact and moderate-impact information resources.
- Develop risk-based plans for information security applicable to networks, facilities and information systems.
- Develop processes for:
    a. Planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the university.

   b. Justifying, granting, and documenting any exceptions to specific program requirements in accordance with TAC.
- Facilitate the development of policies, standards and procedures that include controls for:
   a. Data security risk management required by TAC.
   b. Mitigation of information security risks to levels acceptable to the President.
   c. Information security throughout the life cycle of the information resource.

By approving the security program document, management affirms its support for the information security policies, roles, practices, and other program components necessary to achieve security, consistent with business requirements, relevant laws, and regulations.

General information security policy statements

Lamar University must:

- Protect information resources based on risk against accidental or unauthorized disclosure, modification, or destruction and assure the confidentiality, integrity, and availability of university data.
- Appropriately reduce the collection, use, or disclosure of confidential information contained in any medium, including paper records.
- Apply appropriate physical and technical safeguards without creating unjustified obstacles to the operation of the business and research at the university and the provision of services to its many affiliates.
- Comply with applicable state and federal laws, executive orders and TSUS rules governing information resources.
- Ensure that all capital planning and investment requests include the resources needed to implement the information security program and document all exceptions to this requirement and that information security resources are available for expenditure as planned.
- Develop an enterprise architecture with consideration for information security and the resulting risk to institutional operations, institutional assets, individuals, and other organizations.

Scope

This information security program applies to any person granted access to Lamar University information resources, including but not limited to students, faculty, staff, alumni, temporary employees, contractors, volunteers, friends of Lamar University and guests. Such information resources include but are not limited to data, images, text and software stored on hardware or other digital storage media, both on-campus and at out-sourced locations.

Governance, Role Descriptions and Responsibilities

Governance consists of the leadership and organizational structures to ensure that Lamar University's information resources sustain and extend the university's strategies and objectives.

Lamar University maintains a coordinated approach to the protection of information resources and repositories of protected information that are directly or indirectly under its custody, by establishing appropriate and reasonable administrative, technical and physical safeguards. These safeguards are to be adhered to by all individuals that administer, install, maintain, contract or make use of Lamar University's information resources.

IT governance is the responsibility of executive management with presidential responsibility for information resources. The Vice President of Information Management Decision Support (IMDS) division is a member of executive management, providing strategic direction, ensuring objectives are achieved, ascertaining that risks are managed appropriately, and verifying that Lamar University's information resources are used responsibly.

The IMDS division is responsible for developing, recommending, implementing and monitoring appropriate controls to reduce risk and promoting awareness of IT security requirements and plans throughout Lamar University.

The following roles are subsequently designated with appropriate responsibilities and authorities regarding information resource security, in accordance with TAC 202: Institution head, Information Resource Manager (IRM), Information Security Officer (ISO), IT Compliance, Information Owner/Data Owner, Information Custodian/Data Custodian, User/Information User/Authorized User, IT Steering Committee, Academic Technology Committee, Application Security Committee, Audits and Analysis, and IT Compliance office.

Institution Head/Agency Head

The President of Lamar University is the top-most senior executive with operation accountability for Lamar university. The president is ultimately responsible for the security of information resources. Responsibilities of the President under TAC §202.70 include:

- Designating an Information Security Officer who has the explicit authority and the duty to administer the information security requirements of TAC institution wide.
- Allocating resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the President.
- Ensuring that senior university officials and information-owners, in collaboration with the information resources manager and information security officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect control.
- Ensuring that the university has trained personnel to assist in complying with the requirements of TAC and related policies.
- Ensuring that senior university officials support the university Information Security Officer in developing, at least annually, a report on institution of higher education information security program, as specified in TAC §202.71(b)(11) and §202.73(a).
- Approving high level risk management decisions as required by §202.75(4).
- Reviewing and approving at least annually, institution of higher education information security program, required under §202.74.
- Ensuring that information security management processes are part of the institution of higher education strategic planning and operational processes.

Information Resource Manager (IRM)

The Vice President of IMDS division is designated, through appointment of the President, as Lamar University's IRM. The IRM, as defined by the State of Texas, oversees the acquisition, and use of information resources within the university. The IRM is responsible for the university's information resource planning, budgeting, and performance, including information security components. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies. The IRM is a member of the President's executive management and reports directly to the President.

Information Security Officer (ISO)/Director of IT Systems Security

The Director of IT Systems Security is designated as Lamar University's Information Security Officer (ISO). The ISO reports directly to the IRM, who is part of executive level management. The ISO has authority for information security for the entire university. The ISO is authorized to issue exceptions to information security requirements or controls in TAC, with the approval of the President and to justify, document and communicate any such exceptions as part of the risk assessment process.

The ISO responsibilities under TAC §202.71 and §202.73 include:

- Developing and recommending a campus-wide information security program.
- Developing and maintaining a campus-wide information security plan.
- Developing and maintaining information security policies and procedures that address the requirements of TAC and the University's information security risks.
- Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of TAC and the university's information security risks.
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities.
- Providing guidance and assistance to senior University officials, information owners, information custodians, and end users concerning their responsibilities under TAC.
- Ensuring that annual information security risk assessments are performed and documented by information-owners.
- Reviewing the inventory of information systems and related ownership and responsibilities.
- Developing and recommending policies and establishing procedures and practices, in cooperation with the IRM, information owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.
- Coordinating 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.
- Verifying that security requirements are identified, and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data.
- Reporting, at least annually, to the President, the status and effectiveness of security controls; and inform the campus departments, data owners and data custodians in the event of noncompliance with TAC and/or with Lamar's information security policies.

Information Owner / Data Owner

A data owner is defined as a person(s) with **statutory or operational authority** for specific information or information resources. The data owner or his or her designated representative(s) are responsible for and authorized under TAC §202.72 to:

- Classify information under their authority, with the concurrence of the President or his or her designated representative(s), in accordance with Lamar University's established information classification categories.
- Approve access to information resources and periodically review access lists based on documented risk management decisions.
- Formally assign custody of information or an information resource.
- Coordinate data security control requirements with the ISO.
- Convey data security control requirements to custodians.
- Provide authority to custodians to implement security controls and procedures.
- Justify, document, and be accountable for exceptions to security controls.
- Coordinate and obtain approval for exceptions to security controls with the university's Information Security Officer.
- Participate in risk assessments.

Information Custodian / Data Custodian

An information custodian is defined as a department, agency, or third-party service provider responsible for **implementing the information owner-defined controls** and access to an information resource. Data custodians of information resources, including third party entities providing outsourced information resources services to Lamar University under TAC §202.72 shall:

- Implement controls required to protect information and information resources based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the information security program (ISP).
- Provide owners with information to evaluate the cost-effectiveness of controls and monitoring.
- Adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents.
- Provide information necessary to provide appropriate information security training to employees.
- Ensure information is recoverable in accordance with risk management decisions.
- Participate in risk assessments.

In modern information systems management, the role of data custodianship is a distributed responsibility between university staff, departments, and vendors. The role of custodianship will vary based on the information system and its architecture. For information systems that house, or process confidential information hosted in the university's information processing facilities, the custodianship is the responsibility of Executive Director of IT Operations.

User / Information User / Authorized User

An information user is defined as an individual, process, or automated application authorized to access an information resource in accordance with federal and state law, university policy, and the information owner's procedures and rules. The user of an information resource has the responsibility to:

- Use the resource only for the purpose specified by the institution or information owner.
- Comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction.
- Formally acknowledge that they will comply with the security policies and procedures in a method determined by the President or IRM.

IT Steering Committee and Academic Technology Committee

The two university standing committees which review and recommend university-wide policies regarding information security and privacy assurance.

Audits and Analysis / IT Auditor

The office of internal audit is independent of the information security program. They are designated by the Texas State University System Board of Regents and are responsible for reviewing the

university's information security program at least biennially, for compliance with TAC standards, based on business risk management decisions. The review provides the basis for corrective action plans which further influence the development of policies, procedures, and processes.

IT Compliance office

The office of IT compliance is responsible for facilitating processes that provide central oversight of all information technology acquisitions such that security, privacy, accessibility, and contractual requirements can be satisfied to comply with applicable university policies, state and federal laws and executive orders.

Program Management Components

Risk Management

Risk management is the cornerstone of information security with the goal of reducing risk. Lamar University has adopted the NIST framework (described below) for risk management. The NIST risk management framework allows flexible yet methodic management of risks to information systems. The NIST framework describes risk management along with its institutional value as follows:

> Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.
>
> With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. *

*Retrieved from: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

The risk management cycle described here largely focuses on the business process tier and information systems tiers of NIST-800-93 guidance for enterprise risk management.

Risk management is a 6-step process.

Step1: Categorize the systems and the information processed, stored, and transmitted by the system based on impact analysis.

Step2: Select an initial set of baseline security controls for the system, based on security categorization; tailoring and supplementing the security control baseline as needed, based on assessment of risk and other conditions.

Step3: Implement the security controls and document how the controls are deployed within the system and environment of operation.

Step4: Assess the security controls using appropriate procedures to the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Step5: Authorize system operation based upon a determination of the risk to organizational operations and assets, individuals, resulting from the operation of the system and the decision that this risk is acceptable.

Step6: Monitor and assess selected security controls in the system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of

operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate officials.

In compliance with TAC §202.75 risk assessment activities will result in the following:

- The inherent impact will be ranked, at a minimum, as either "High," "Moderate," or "Low".
- Information systems categorized high must be assessed for risk annually, information systems categorized moderate must be assessed for risk biennially, and information systems categorized low must be assessed for risk every three years, unless a substantial change in the system state or data triggers a re-categorization.
- Risk assessment results, vulnerability reports, and similar information must be documented and presented to the Information Security Officer or his or her designated representative(s).
- Approval of the security risk acceptance, transference, or mitigation decisions shall be the responsibility of:
    a. the information security officer or his or her designee(s), in coordination with the information owner, for systems identified with Low or Moderate residual risk.
    b. the President for all systems identified with a residual High Risk.

Additional operational details on managing risks are documented in the risk management policy and procedures.

Information systems inventory

Before an information system can be secured it needs to be “known” to the risk governance process. To facilitate proper management of information assets the office of the IRM is responsible for maintaining an inventory of information systems.

Information security workforce

In compliance with state of Texas guidelines, the Information Security Office is authorized to facilitate programs focused on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

Information Security Measures of Performance

In compliance with state of Texas guidelines, the Information Security Office is authorized to develop, monitor, and report to executive leadership on the results of information security measures of performance.

Testing, training, and monitoring

The Information Security Office is responsible for providing oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. In particular, the office of ISO must implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with information systems are developed, maintained, and executed continuously.

Contacts with security groups and associations

Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Based on organizational missions/business functions, university security staff are encouraged to share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Threat awareness and information-sharing

Because of the constantly changing and increasing sophistication of adversaries, especially the Advanced Persistent Threat (APT), it is becoming more likely that adversaries may successfully breach or compromise information systems. One of the best techniques to address this concern is for the University to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that we have experienced, mitigations that are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur).

The information security workforce at the university are encouraged to take part in information sharing activity with peers and other entities at federal, state and system (TSUS) levels.

Governance documentation

This document primarily focuses on the information security program and its associated program management controls. The Texas control catalog, based on NIST SP 800-53, lists controls for institutions of higher education to provide specific guidance for implementing security protocols. These controls include organizational, physical and technical controls.

To simplify the adoption and enforcement of controls, organizational controls are grouped into policy documents. Physical and technical controls are grouped separately into the Lamar Technical Control Index. The table below provides a mapping of the university's documents that topically cover Texas control catalog families.

	NIST / DIR control family	**Regulatory Document**	**Lamar University Policy Mapping**	**Lamar University Document number**
TSUS	IA	Appendix - IA - Identification and Authentication.docx	Information Systems Management Policy	10.01.01
	AC	Appendix - AC - Access Control.docx		

	AU	Appendix - AU - Audit and Accountability.docx		
	MA	Appendix - MA - Maintenance.docx		
	SI	Appendix - SI - System and Information Integrity.docx		
	MP	Appendix - MP - Media Protection.docx		
	SC	Appendix - SC - System and Communications Protection.docx		
	CM	Appendix - CM - Configuration Management.docx		
	CP	Appendix - CP - Contingency Planning.docx		
	SA	Appendix - SA - System and Services Acquisition.docx	System and Service Acquisition Policy	10.01.02
	PE	Appendix - PE - Physical and Environmental Protection.docx	Physical and Environmental Protection Policy	10.01.03
	AT	Appendix - AT - Awareness & Training.docx	Awareness and training Policy	10.01.04
	PL	Appendix - PL - Planning.docx	Risk management Policy	10.01.05

	CA	Appendix - CA - Security Assessment and Authorization.docx		
	RA	Appendix - RA - Risk Assessment.docx		
	PM	Appendix - PM - Program Management.docx	Information Security Program (this document)	05.01.01
	IR	Appendix - IR - Incident Response.docx	Incident Management Policy	10.01.07
	PS	Appendix - PS - Personnel Security.docx	Acceptable Use/Appropriate Use and Transparency, Use Limitation Policy & HR policies	10.01.08
		Appendix - Network Management.docx	Network Management Policy	10.01.09
		Appendix - Server Management.docx	Server Management Policy	10.01.10
Texas DIR	AP	Texas Control Catalog v1.3 - Authority and Purpose	Privacy Policy	10.02.01
	DI	Texas Control Catalog v1.3 - Data Quality and Integrity		
	DM	Texas Control Catalog v1.3 - Data Minimization and Retention		
	AR	Texas Control Catalog v1.3 - Accountability, Audit, Risk Management		

	IP	Texas Control Catalog v1.3 - Individual Participation and Redress		
	SE	Texas Control Catalog v1.3 - Security		
	TR	Texas Control Catalog v1.3 - Transparency		
	UL	Texas Control Catalog v1.3 - Use Limitation		

Appendix

Compliance references

Lamar University information security program and practices must comply with several federal and state laws, TSUS rules and regulations and Lamar University policies. While it is not possible to list all potentially applicable laws and regulations, this list references the most relevant ones that must be complied.

1. Texas State University System Rules and Regulations
2. The Federal Family Educational Rights and Privacy Act (FERPA)
3. Health Insurance Portability and Accountability Act (HIPAA)
4. Federal Information Security Management Act (FISMA)
5. Texas Administrative Code, Title 1, part 10, Chapter 202, Subchapter C
6. Texas Security Controls Standards Catalog
7. Texas Administrative Code, Title 1, part 10, Chapter 203
8. Texas Government Code, Chapter 2054 – Information Resources
9. Texas Government Code, Chapter 2059 – Texas Computer Network Security System
10. Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
11. Texas Penal Code, Chapter 33 – Computer Crimes
12. Digital Millennium Copyright Act
13. Copyright Act of 1976

REVISION AND RESPONSIBILITY

This section is to be completed by the IT Policy Manager

Oversight Responsibility: IMDS Division

Review Schedule: Every two years

Last Review Date: 7/6/2021

Next Review Date: 6/7/2023

APPROVAL

This section is to be completed by the IT Policy Manager

_____ 7/6/2021

President, Lamar University **Date of Approval**

_____ 7/6/2021

IRM, Lamar University **Date of Approval**

REVISION HISTORY

Revision Number	Approved Date	Description of Changes
1	12/15/2015	Initial Version
2	1/19/2016	Amended numbering convention by replacing "10.01.01" to "05.01.01."
3	6/7/2021	Updated IRM title to IMDS. Updated program components to align with PM control family from Texas control catalog. Moved definitions to Definition Catalog. Added policy mapping table. Changed signature authority from CIO to IRM. Defined risk management as part of Information Security Program.