INFORMATION TECHNOLOGY
LAMAR UNIVERSITY

DOCUMENT NAME INFORMATION SECURITY PROGRAM
EFFECTIVE DATE January 1, 2016

Executive Summary

An information security program (ISP) is designed to protect information 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.

The information security program (ISP) governs the confidentiality, integrity and availability of Lamar University data, especially highly sensitive or critical data, and defines the 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 defines information security standards for institutions of higher education. The rules in TAC 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 the purpose, scope, governance structures, authority, organizational responsibilities and foundational elements of the information security program for Lamar University.

Table of Contents

Introduction

This document establishes Lamar University's information security program (ISP) as mandated by Texas Administrative Code (TAC) 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.

Where applicable, policies, procedures, standards, guidelines and controls will be 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 of hardware and software functions.

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

Purpose

The purpose of the information security program is to:

1. ensure the confidentiality, integrity, and availability of Lamar University data;
2. satisfy and maintain compliance with applicable laws, codes, controls, rules and regulations;
3. reflect Lamar University's commitment to stewardship of sensitive and critical business information;
4. establish the governance and responsibilities for information security at Lamar University;
5. 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;
6. provide for information classification and establish controls for each classification type;
7. establish an ongoing security awareness education program for all users starting with new employees during onboarding process;
8. establish strategies to protect high-impact information resources;
9. develop risk based plans for information security applicable to networks, facilities and information systems;
10. develop processes to:
    a. plan, implement, evaluate, and document remedial action to address any deficiencies in the information security policies, procedures, and practices of Lamar University; and
    b. justify, grant and document any exceptions to specific program requirements in accordance with requirements and processes defined in TAC;

11. 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; and
    c. information security throughout the life cycle of the information resource.

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 who have access to Lamar University information resources. Such technology resources include but are not limited to data, images, text and software which are stored on hardware or other digital storage media both on-campus and at out-sourced locations.

Governance and Responsibilities

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

Lamar University will maintain a coordinated approach to the protection of information resources and repositories of protected information that are directly or indirectly under Lamar University's 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 IT/Chief Information Officer (CIO) is a member of executive management, provides strategic direction, ensures objectives are achieved, ascertains that risks are managed appropriately, and verifies that Lamar University's information resources are used responsibly.

The IT division is responsible for developing and implementing controls and promoting awareness of IT security requirements and plans throughout Lamar University.

The following roles are subsequently defined with appropriate responsibilities and authorities regarding information security:

- 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; and
- ISP Reviewer.

Information Resource Manager (IRM)/Chief Information Officer (CIO)

The Vice President of IT is designated through appointment of the President, as Lamar University's CIO/IRM. The IRM, as defined by the State of Texas, oversees the acquisition and use of information resources within Lamar University. The IRM is responsible for Lamar 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, reports directly to the President, and is the designated representative for the University's information resources.

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. The ISO has authority for information security for the entire university.

The ISO is responsible to:

- develop and recommend a campus-wide information security program as required by TAC;
- develop and maintain a campus-wide information security plan;
- develop and maintain information security policies and procedures that address the requirements of TAC and the University's information security risks;
- work 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;
- train and oversee personnel with significant responsibilities for information security with respect to such responsibilities;
- provide guidance and assistance to senior University officials, information owners, information custodians, and end users concerning their responsibilities under TAC;
- ensure that annual information security risk assessments are performed and documented by information-owners;
- review the inventory of information systems and related ownership and responsibilities;
- develop and recommend policies and establish 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;
- 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;
- verify 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;
- report 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; and
- issue exceptions to information security requirements or controls in TAC, with the approval of the President. Justify, document and communicate any such exceptions as part of the risk assessment process.

IT Compliance/Director of IT Compliance

The Director of IT Compliance is responsible for recommending and developing an appropriate, structured methodology to help identify, evaluate and minimize risks related to the information resources that support Lamar University's mission. This office, with the aid of other departments, will coordinate periodic technology risk assessments.

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 to:

- classify information under their authority, with the approval 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 (including implementation and review of) 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; and
- participate in risk assessments.

Information Custodian / Data Custodian

An information custodian is defined as an individual, a department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource. This responsibility typically falls on administrators of applications and systems for shared information resources such as servers. Users assume the role of data custodians of Lamar University data that is under their possession on their computing devices, portable storage and cloud storage locations. Data custodians of information resources, including third party entities providing outsourced information resources services to Lamar University 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; and
- ensure information is recoverable in accordance with risk management decisions.

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, agency 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; and
- 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 IT Steering Committee and Academic Technology Committee are standing committees which review and recommend university-wide policies regarding information security and privacy assurance.

Application Security Committee

The Application Security Committee is a committee of data custodians, data owners, and their delegated operational representatives chaired by the Information Security Officer (ISO).The Application Security Committee serves as a platform and a conduit between designated data owners and data custodians of Lamar University with reference to application security.

Information Security Program Reviewer

The Information Security Program is reviewed by individual(s) designated by the President that are independent of the program. The review is conducted at least biennially for compliance with TAC standards based on business risk management decisions. The office of audits and analysis may be called upon to assist in the review process. Outcomes of the review provides the basis for corrective action plans and the development of policies, procedures and processes.

Foundational elements of ISP framework

The following foundational elements are designed to create a framework for the information security program (ISP), help Lamar University adopt a control catalog, and comply with Texas Administrative Code (TAC). The description of each element includes a definition, description of primary activities, and assignment of responsibility. The 10 foundational elements of the information security program are:

- accountability of information assets;
- classification of data;
- data risk management;
- identity and access management;
- control activity;
- security awareness;
- physical security;
- contingency planning;
- security incident response; and
- data disposition.

These elements may be reviewed and updated every two years consistent with the State of Texas reporting cycle or when the environment and/or regulations change.

Element 1: Inventory and accountability of information assets

Lamar University departments collect, store and use various data as part of normal business operations. These are stored in various information systems. An inventory of these information systems, data owners, and data custodians is required.

Activity Description	Assigned Responsibility
Inventory of systems, data owners and data custodians	IT Compliance and ISO
Periodic review of access and authorization granted	Data owners
Implement controls	Data custodians
Respond to audits and inquiries	Data owners and custodians
Acknowledge policies and confidentiality	Authorized users

Element 2: Classification of data

Information classification (data classification) is required to determine the relative sensitivity and criticality of information resources, which provides the basis for protection efforts and access control.

Lamar University adopts a four-category classification: regulated, confidential, sensitive and public, as defined by TAC. Although all data requires some level of protection, particular data classifications are considered more sensitive and require tighter controls. The level of security required depends in part on the effect that unauthorized access or disclosure of data would have on operations, functions, reputation, assets, or privacy of individual members of the Lamar University community.

The Data Classification Standard outlines the minimum controls for protection of classified Lamar University information. Additional controls may be required under applicable laws, regulations or standards governing specific types of data (e.g., health or financial information, credit card data).

Activity Description	Assigned Responsibility
Develop and maintain data classification policy and standard	ISO
Develop and maintain applicable control standards	ISO
Classify data	Data owners
Implement controls	Data custodians

Element 3: Data risk management

Data risk management is the process of aligning information resource risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures. The risk management cycle includes assessment, review, mitigation and reporting. It includes the following activites.

- Risk assessment is the process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls. Risk assessment also provides the documentation for evaluating and granting exemptions from security control requirements.
- Risk review is the process of evaluating the results of risk assessments and recommending activities to mitigate the risks.
- Risk mitigations are technical and/or procedural activities designed to reduce or eliminate the risks identified during assessment and review.
- Risk reporting is the process of reporting residual risks to the President and executive administration.

Activity Description	Assigned Responsibility
Coordinate risk assessment activities	IT Compliance
Participate in risk assessment	Data owners and data custodians
Review assessment results and recommend remediation requirements	ISO
Mitigate identified risks	Data custodians
Grant exemptions to controls requirements based on risk assessments	ISO
Residual risk reporting	ISO

Element 4: Identity & Access Management (IAM)

Identity and access management ensures accurate identification of authorized users and provides secure authorized access to the use of information resources. The purpose of identity management is to:

- ensure unique identification of users;
- assign access privileges based on identity; and
- maintain effective identity mechanisms through evolving technologies and regulations.

Access control refers to the process of controlling access to systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of Lamar University's information assets. Access control measures include secure and accountable means of identification, authentication and authorization. These measures include the following:

- assign access privileges to authenticated users;
- allow user access to information resources granted only by authorized individuals;
- ensure periodic review of users and their access; and
- maintain effective access mechanisms through evolving technologies and regulations.

Activity Description	Assigned Responsibility
IAM policy development and maintenance	IRM or designee
IAM technology standards development and maintenance	IRM or designee
IAM procedure development and maintenance	IRM or designee

Element 5: Control activity

Defined controls provide a system of checks and balances intended to identify irregularities, prevent abuse from occurring, and assist in resolving discrepancies that are introduced into the operation of the business. Control activities and mechanisms help ensure remediation requirements are carried out to reduce risks identified during the risk assessment process.

The Texas Department of Information Resources (DIR) has published a Security Controls Standards Catalog (SCSC) for the purpose of providing state agencies and higher education institutions specific guidance for implementing security controls in a format that easily aligns with the National Institute of Standards and Technology Special Publication 800-53 Version 4 (NIST SP 800-53 Rev. 4). The control catalog specifies the minimum information security requirements that state organizations must use to provide the appropriate levels of information security according to risk levels.

Activity Description	Assigned Responsibility
Develop and maintain information security plan that tracks adoption of appropriate security controls	ISO
Report effectiveness of security controls	ISO
Submit information security plan to DIR biennially	ISO
Coordinate data security control requirements with the ISO and convey them to data custodians	Data owners
Implement controls	Data custodians

Element 6: IT security awareness

Security awareness is a critical component of an information security program. The goal of the information security awareness program is to strengthen the information security culture of Lamar University through education, active learning, communication and collaboration. The information security awareness program will enhance stakeholder awareness of potential threats to Lamar University's information resources.

Activity Description	Assigned Responsibility
Maintain and operate an ongoing security awareness program	ISO
Coordinate development and effective maintenance of communication and internal marketing strategies for information security awareness	ISO
Participate in security awareness program	All users

Element 7: Physical security

Physical security controls and secure areas are used to minimize unauthorized access, damage, and interference to information resources. This includes providing environmental safeguards and controlling physical access to equipment and Lamar University data consistent with TAC and State Office of Risk Management rules and guidelines.

Activity Description	Assigned Responsibility
Develop and maintain physical security policies	IRM or designee
Implement physical security procedures	Data custodians

Element 8: IT contingency planning

IT contingency planning (CP) ensures that mission-critical business functions identified in the campus business continuity plan (BCP), which require IT resources, are addressed. The BCP ensures that the effects of a disaster will be minimized and Lamar University will be able to either maintain or quickly resume mission-critical functions.

Elements of the written BCP for information resources shall include:

- Business Impact Analysis: The analysis shall include the following:
  - Mission Critical Information Resources;
  - Disruption impacts and allowable outage times; and
  - Recovery priorities;
- Risk Assessment;
- Implementation, testing, and maintenance management program for the plan; and
- Disaster Recovery Plan.

Activity Description	Assigned Responsibility
Develop and maintain BCP	IT Compliance
Develop and maintain applicable policy, process and procedures	IT Compliance
Coordinate distribution of BCP	IT Compliance
Implement and test of BCP	IRM or designee

Element 9: Information security incident response

An information security incident is defined as an event that impacts or has the potential to impact the confidentiality, availability or integrity of Lamar University information resources. Having an effective incident response plan is essential in mitigating damage and loss. Proper handling of such incidents protects Lamar University's information resources from future unauthorized access, misuse or damage.

Activity Description	Assigned Responsibility
Develop and maintain incident response policy	ISO
Coordinate incident response activities	ISO
Develop and maintain of incident response plan	ISO
Develop and maintain incident response procedures for: • incident management; • user reporting; and • State reporting.	ISO

Element 10: Digital data disposition

The secure disposal of Lamar University's digital data is a significant part of the information security posture. Lamar University data can be stored on both printed media and on digital format. It is vital both these forms of data are disposed of securely to ensure confidentiality. In order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality, specific disposition methods for digital data must be adhered to.

Activity Description	Assigned Responsibility
Develop and maintain data disposition policy and standards	ISO
Implement data disposition standards	Data custodians

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. Security Controls Standards Catalog published by Texas Department of Information Resources
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

Definitions

Availability – Ensuring that information systems and the necessary data are accessible for use when required.

Business Continuity Plan - A plan to ensure that the essential business functions of the organization are able to continue (or re-start) in the event of unforeseen circumstances. This is also known as written continuity of operations plan (WCOP).

Confidentiality – Assurance that information is shared only among authorized persons or organizations.

Disaster Recovery Plan – Assurance that a documented process or set of procedures to recover and protect a business IT infrastructure is in place in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster.

Information Resource – Defined in §2054.003(7), Government Code and/or other applicable state or federal legislation as follows:

Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.*

*Modification of this definition through state or federal legislation shall supersede the above.

Information Resources of Lamar University include, but are not limited to the following:

- all components of the Lamar University information network, both physical and logical;
- any device owned by Lamar University or used to connect to the Lamar University network. These devices include computers (both stationary and mobile), printers, and communication devices;
- all software purchased by or used to support Lamar University;
- all electronic data, including email, and the storage media on which the data resides (both stationary and mobile); and
- Lamar University credentials used to access licensed external resources.

Information Security – The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information Security Program – Program that contains administrative, technical, and physical safeguards to protect information resources.

Integrity –Accuracy and consistency of data over the entire life-cycle.

Mitigate – An effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Remediate – The act or process of correcting a fault or deficiency.

Risk – The likelihood that something will occur and cause harm to, or loss of, an information asset.

Risk Assessment – A systematic process of evaluating potential risk and impact from disruption of information resources.

Security Incident - A computer, network, or paper based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

Threat – Anything that has the potential to cause harm.

Vulnerability – A weakness that could be exploited to endanger or cause harm to an information resource.

Vulnerability Assessment - The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

REVISION AND RESPONSIBILITY

Oversight Responsibility: IT Division

Review Schedule: Every three years

Last Review Date: December 15, 2015

Next Review Date: December 15, 2018

APPROVAL

Kenneth Evans — December 15, 2015
President, Lamar University — **Date of Approval**

Priscilla Parsons — December 15, 2015
Chief Information Officer, 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.”