Information Resources
Policy Manual

Lamar State College Port Arthur

Member Texas State University System™

April 2024

PREFACE

The *Information Resources Policy Manual* applies to all users of Lamar State College Port Arthur information resources, including faculty, staff, students, and others with authorized computing accounts.

Policies and procedures outlined in this document may be amended at any time.

Questions about this policy should be addressed to the LSCPA Information Resources Manager at irm@lamarpa.edu.

TABLE OF CONTENTS

POLICY: 1.0 INFORMATION RESOURCES MANAGEMENT
SCOPE: FACULTY, STAFF, AND STUDENTS
APPROVED: November 2020
REVISED:

1.1. Policy Statement

Lamar State College Port Arthur's (LSCPA) information resources are vital academic and administrative assets which require appropriate safeguards to avoid compromising their confidentiality, integrity, and availability. As a public higher institution of education, LSCPA is subject to various federal, state, and industry regulations that provide requirements and guidance for achieving this goal.

The purpose of this policy is to establish the framework on which LSCPA's information resources policies, standards, guidelines, and procedures are created and maintained.

1.2. Definitions

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

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

1.3. Roles and Responsibilities

1.3.1. President

1.3.1.1. The President may delegate some or all the operational duties in Section 1.3.1.2.

1.3.1.2. The President or designated representative shall:

1.3.1.2.1. Designate an Information Resources Manager (IRM) as required by Texas Government Code §2054.071, with the mission and resources to coordinate, implement, and maintain the College's information resources.

1.3.1.2.2. Ensure that College personnel cooperate as necessary with the IRM to enable the IRM to perform their duties.

1.3.1.2.3. Appoint an Information Security Officer (ISO) with the mission and resources to coordinate, develop, implement, and maintain a College-wide information security program.

1.4. Information Resources Manager (IRM)

1.4.1. The IRM has authority and oversight over the College's information resources and use of information technology.

1.4.2. The IRM is part of the College's executive management.

1.4.3. The IRM reports directly to the Executive Vice President of Finance and Operations.

1.4.4. The IRM has the following responsibilities:

1.4.4.1. Preparing information resources operational reports in accordance with Texas Government Code §2054.074.

1.4.4.2. Overseeing the implementation of the College's project management practices as they relate to information resources.

1.4.4.3. Overseeing and approving the College's acquisition and use of information technology.

1.4.4.4. Maintaining information resources policies as described in Section 1.8 of this policy.

1.4.4.5. The IRM must maintain relevant knowledge and skills by participating in continuing professional education activities in accordance with the guidelines established by the Texas Department of Information Resources.

1.5. Information Security Officer (ISO)

1.5.1. The ISO has authority over information security for LSCPA.

1.5.2. The ISO reports directly to the Executive Vice President for Finance and Operations.

1.5.3. The ISO must possess the appropriate training and experience required to administer the functions described the College's information resources policies.

1.5.4. The ISO's primary duties are related to information security.

1.6. Information Technology Services Department

1.6.1. LSCPA's Information Technology Services department (ITS) is responsible for maintaining information resources standards, guidelines, and procedures as described in Section 1.8 of this policy.

1.7. General

1.7.1. Documentation for LSCPA's information resources policy framework is separated into four (4) categories of documentation: policies, standards, guidelines, and procedures.

1.7.2. Information resources policies shall be managed formally as described in Section 1.81.8 of this policy.

1.7.3. If standards, guidelines, or procedures are included in policy documents, they are also subject to the same policy management process as described in Section 1.8 of this policy.

1.7.4. Standards, guidelines, or procedures referenced by policies but not directly included in policy shall be managed as described in Section 1.9 of this policy.

1.8. Information Resources Policy Management

1.8.1. New and revised information resources policies shall originate from the IRM, the Information Security Officer (ISO), or a designated committee.

1.8.2. The review and approval process is as follows:

1.8.2.1. Policies must be reviewed by the ISO prior to being submitted for approval.

1.8.2.2. Policies must be reviewed by the IRM prior to being submitted for approval.

1.8.2.3. LSCPA has the option to forward the policy to general counsel, human resources, or other appropriate entities for review.

1.8.2.4. Policies must be reviewed by executive management and LSCPA's President grants final approval.

1.8.3. Minor revisions to existing information resources policies shall originate from the IRM. Minor revisions include changes to the numbering sequence, minor grammatical edits, formatting changes, and updates to hyperlinks. These changes do not require approval under the process described in Section 1.8.2 of this policy.

1.8.4. Information resources policies shall be reviewed and updated every 3 years at a minimum. Review of policies may also be triggered by changes to Texas State University System policies, federal and state laws, and other regulatory requirements.

1.8.5. Unit procedures derived from information resources policies shall be reviewed annually and revised as necessary.

1.9. Information Resources Standards, Guidelines, and Procedures Management

1.9.1. New and revised standards, guidelines, and procedures shall originate from the IRM, the ISO, or the Information Technology Services department.

1.9.2. New and revised standards, guidelines, or procedures that impact only the Information Technology Services department require only the IRM's approval.

1.9.3. New and revised standards, guidelines, or procedures that impact other units or the College as a whole require the timely approval of executive management.

1.9.4. Minor revisions to existing standards, guidelines, and procedures require approval only from the IRM. Minor revisions include changes to the numbering sequence, minor grammatical edits, formatting changes, and updates to hyperlinks.

1.9.5. Standards, guidelines, and procedures must be reviewed by the Information Technology Services department annually and revised as necessary.

1.10. Related Policies, Regulations, Standards, and Guidelines

1.10.1. 1 Tex. Admin. Code § 202.70

1.10.2. 1 Tex. Admin. Code § 202.71

1.10.3. Texas Government Code §2054 Subchapter D

1.10.4. LSCPA Information Resources Policy 5.0 Information Security Program

POLICY: 2.0 APPROPRIATE USE OF INFORMATION RESOURCES
SCOPE: FACULTY, STAFF, AND STUDENTS
APPROVED: November 2020
REVISED:

2.1. Policy Statement

Lamar State College Port Arthur recognizes the importance of information resources and facilities to students, faculty, and staff. This policy establishes the appropriate use of information resources in order to:

2.1.1. achieve College-wide compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

2.1.2. establish prudent and appropriate practices regarding the use of information resources; and

2.1.3. educate individuals about the responsibilities they assume when using Lamar State College Port Arthur's information resources.

2.2. Applicability

2.2.1. Applicable College policies and procedures include all LSCPA policies and procedures that address the usage of LSCPA information resources. Also applicable are College policies prohibiting harassment, plagiarism, or unethical conduct.

2.2.2. Laws that apply to the use of LSCPA's information resources include laws pertaining to theft, copyright infringement, insertion of malicious software into computer systems, and other computer-related crimes.

2.2.3. This policy applies to all College information resources, regardless of where they reside.

2.3. General

2.3.1. LSCPA provides each of its authorized users with a computer account, known as an LSCPA User ID, which facilitates access to the LSCPA's information resources. In accepting an LSCPA User ID or any other access ID, the recipient agrees to abide by applicable LSCPA policies and federal, state, and local laws. LSCPA reserves the right at any time to limit, restrict, or deny access to its information resources and to take disciplinary or legal action against anyone in violation of these policies or statutes.

2.3.2. LSCPA provides information resources for the purpose of accomplishing tasks related to the College's mission. LSCPA expects its faculty and staff to employ these resources as their first and preferred option for satisfying their business, research, or instructional needs.

2.3.3. The College may restrict the use of or access to its information resources.

2.3.4. LSCPA's computer information resources are not a public forum.

2.3.5. LSCPA considers email a significant information resource and an appropriate mechanism for official College communication. The College provides official College email addresses and services to its students, faculty, staff, and organizational units for this purpose and to enhance the efficiency of educational and administrative processes. In providing these services, the College anticipates that email recipients will access and read College communications in a timely fashion.

2.3.6. Subject to applicable College policies and procedures, students are allowed to use the College‘s information resources for school-related purposes.

2.3.7. Employees of LSCPA are allowed to use the College‘s information resources in the performance of their job duties and must adhere to all applicable College policies and federal, state, and local laws. State law and College policy permit incidental personal use of LSCPA information resources, subject to review and reasonable restrictions by the employee's supervisor.

2.3.8. Censorship is not compatible with LSCPA's goals. The College will not limit access to any information due to its content, as long as it meets the standard of legality. The College reserves the right, however, to impose reasonable time, place, and manner restrictions on expressive activities that use its information resources. Furthermore, the College reserves the right to block or impose necessary safeguards against files and other information, such as malicious software and phishing emails, that are inherently malicious or pose a threat to the confidentially, integrity, or availability of information resources for the College and its stakeholders.

2.3.9. LSCPA's information resources are subject to monitoring, review, and disclosure as provided in Information Resources Policy 6.0 Information Security Control Standards, Section 6.16 System and Information Integrity. Consequently, users should not expect privacy in their use of LSCPA's information resources, even in the case of users' incidental, personal use.

2.3.10. Intellectual property laws extend to the electronic environment. Users should assume that works communicated through LSCPA's network infrastructure and other information resources are subject to copyright laws, unless specifically stated otherwise.

2.3.11. The state of Texas and the College consider information resources as valuable assets. Further, computer software purchased or licensed by the College is the property of the College or the company from whom it is licensed. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas and federal statutes.

2.3.12. All policies that apply to College-owned computing devices (e.g., desktop computers, laptop computers, or mobile devices) used on campus also apply to those used off-campus (e.g., home-based computers, mobile devices, or laptop use while travelling), including restrictions on use as listed in Section 2.4 of this policy.

2.4. Inappropriate Uses of Information Resources

2.4.1. The following activities exemplify inappropriate use of the College's information resources. These and similar activities are strictly prohibited for all users:

2.4.1.1. Use of College information resources for illegal activities or purposes. The College will deal with such use appropriately and will report such use to law enforcement authorities. Examples of illegal activities or purposes include unauthorized access, intentional corruption or misuse of information resources, theft, and child pornography.

2.4.1.2. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the College's information resources.

2.4.1.3. The abuse of information resources, including any willful act that:

2.4.1.3.1. endangers or damages any specific computer software, hardware, program, network, data, or the system as a whole, whether located on campus or elsewhere on the global Internet;

2.4.1.3.2. creates or allows a computer malfunction or interruption of operation;

2.4.1.3.3. injects a malicious software into the computer system;

2.4.1.3.4. sends a message with the intent to disrupt College operations or the operations of outside entities;

2.4.1.3.5. produces output that occupies or monopolizes information resources for an unreasonable time period to the detriment of other authorized users;

2.4.1.3.6. consumes an unreasonable amount of communications bandwidth, either on or off campus, to the detriment of other authorized users; or

2.4.1.3.7. fails to adhere to time limitations that apply at computer facilities on campus.

2.4.1.4. Use of College information resources for personal financial gain or commercial purpose.

2.4.1.5. Failure to protect a password or LSCPA ID from unauthorized use.

2.4.1.6. Falsely representing one's identity through the use of another individual's LSCPA User ID or permitting the use of an LSCPA User ID and password by someone other than their owner; this restriction also applies to Personal Identification Numbers (PINs), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes.

2.4.1.7. Unauthorized attempts to use or access any electronic file system or data repository.

2.4.1.8. Unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained on any electronic file, program, network, web page, or College hardware or software.

2.4.1.9. Installing any software on College-owned information resources without Information Technology Services Department approval.

2.4.1.10. Unauthorized duplication, use, or distribution of software and other copyrighted digital materials (including copyrighted music, graphics, videos, etc.). All software and many other digital materials are covered by some form of copyright, trademark, license, or agreement with potential civil and criminal liability penalties. The copyright or trademark holder must specifically authorize duplication, use or distribution, or a specific exception of the Copyright Act, such as the Fair Use exception, the Library exception, or exceptions under the TEACH Act, must apply.

2.4.1.11. Participating or assisting in the deliberate circumvention of any security measure or administrative access control that pertains to College information resources.

2.4.1.12. Using College information resources in a manner that violates other College policies or student code handbook, such as racial, ethnic, religious, sexual, or other forms of harassment.

2.4.1.13. Using College information resources for the transmission of spam mail, chain letters, malicious software (e.g., viruses, worms, or spyware), phishing, or personal advertisements, solicitations, or promotions.

2.4.1.14. Modifying any wiring or attempting to extend the network beyond the port (i.e., adding hubs, switches, wireless access points, or similar devices) in violation of Information Resources Policy 6.0 Information Security Control Standards, Section 6.14.

2.4.1.15. Using LSCPA's information resources to affect the result of a local, state, or national election or to achieve any other political purpose (consistent with Texas Government Code §556.004).

2.4.1.16. Using LSCPA's information resources to state, represent, infer, or imply an official College position without appropriate authorization.

2.4.1.17. Unauthorized network scanning, foot printing, reconnaissance, or eavesdropping on information resources for available ports, file shares, or other vulnerabilities.

2.4.1.18. Unauthorized alteration or relay of network traffic (e.g., man in the middle attacks).

2.4.2. The following restrictions apply to incidental use of College information resources:

2.4.2.1. Incidental personal use of information resources is restricted to College-approved users; it does not extend to family members or other acquaintances.

2.4.2.2. Incidental use must not result in direct costs to the College.

2.4.2.3. Incidental use must not interfere with the normal performance of an employee's work duties.

2.5. Responsibilities of Users

2.5.1. Each user shall utilize College information resources responsibly and respect the needs of other users.

2.5.2. In keeping with LSCPA's core values, all uses of its information resources should reflect high ethical standards, mutual respect, and civility.

2.5.3. Users are responsible for any activity that takes place using their account.

2.5.4. Users must report any suspected weaknesses in computer security, any incidents of possible abuse or misuse, or any violation of this agreement to the Information Technology Services department and/or the ISO immediately upon discovery.

2.5.5. Administrative heads and supervisors must report ongoing or serious problems regarding the use of LSCPA information resources to the Information Technology Services department.

2.5.6. Each user shall immediately notify the Information Technology Services department and/or the ISO of the loss of any fixed or portable storage device or media, regardless of ownership, that contains College data. (See Information Resources Policy 6.0 Information Security Control Standards, Section 6.11.)

2.6. Access to College Information Resources by Auditors

2.6.1. Consistent with Chapter III, paragraph 7.4 of The TSUS Rules and Regulations, the TSUS director of Audits and Analysis and auditors reporting to them, either directly or indirectly, while in the performance of their assigned duties, shall have full, free, and unrestricted access to all College information resources, with or without notification or consent of the assigned owner of the resources. This includes personal information stored on College information resources. The College shall afford this access consistent with Information Resources Policy 6.0 Information Security Control Standards, Section 6.8.

2.6.2. The College shall provide state, federal, and other external auditors with access to College information resources with prior approval by the IRM.

2.7. Consequences for Failure to Adhere to this Policy

2.7.1. Failure to adhere to this policy may lead to the revocation of a user's LSCPA User ID, suspension, dismissal, or other disciplinary action by the College, as well as referral to legal and law enforcement agencies.

2.7.2. Statutes pertaining to the use of College information resources include the following:

2.7.2.1. The Federal Family Educational Rights and Privacy Act (FERPA) – restricts access to personally identifiable information from students' education records.

2.7.2.2. 1 Tex. Admin. Code §202.70-76 – establishes information security requirements for Texas state agencies and public higher education institutions.

2.7.2.3. Texas Penal Code, Chapter 33: Computer Crimes – specifically prohibits unauthorized use of College computers, unauthorized access to stored data, or dissemination of passwords or other confidential information to facilitate unauthorized access to the College's computer system or data.

2.7.2.4. Texas Penal Code, §37.10: Tampering with Governmental Record – prohibits any alteration, destruction, or false entry of data that impairs the validity, legibility, or availability of any record maintained by the College.

2.7.2.5. United States Code, Title 18, Chapter 47, §1030: Fraud and Related Activity in Connection with Computers – prohibits unauthorized and fraudulent access to information resources, accessing a computer to obtain restricted information without authorization; altering, damaging, or destroying information on a government computer without authorization; trafficking in passwords or similar information used to gain unauthorized access to a government computer; and transmitting viruses and other malicious software.

2.7.2.6. Copyright Law, 17 U.S.C. §101-1332, 18 U.S.C. §2318-2323 – forms the primary basis of copyright law in the United States, as amended by subsequent legislation. The Law spells out the basic rights of copyright holders and codifies the doctrine of fair use.

2.7.2.7. Digital Millennium Copyright Act (DMCA), 17 U.S.C. §512 as amended and 28 U.S.C. §4001 – criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. The Act amended Title 17 of the United States Code to extend the reach of copyright, while limiting the liability of internet service providers (like LSCPA) for copyright infringement by their users, provided the service provider removes access to allegedly infringing materials in response to a properly formed complaint.

2.7.2.8. Electronic Communications Privacy Act (U.S.C., Title 18) – prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

2.7.2.9. Computer Software Rental Amendments Act of 1990 – deals with the unauthorized rental, lease, or lending of copyrighted software.

2.7.2.10. Texas Government Code §556.004 – prohibits using state resources or programs to influence elections or to achieve any other political purpose.

2.7.2.11. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R 164 – sets security management requirements and broad management controls to protect the privacy of patient health information.

2.7.2.12. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §3541 – requires every federal agency to develop, document, and implement an agency-wide information security program. The law was amended by FISMA 2010, which changed the focus from paperwork compliance to continuous monitoring and threat mitigation.

2.8. Related Policies, Regulations, Standards, and Guidelines

2.8.1. Computer Software Rental Amendments Act of 1990

2.8.2. Copyright Law, 17 U.S.C. §101-1332, 18 U.S.C. §2318-2323.

2.8.3. Digital Millennium Copyright Act (DMCA), 17 U.S.C. §512 as amended and 28 U.S.C. §4001

2.8.4. Electronic Communications Privacy Act (U.S.C., Title 18)

2.8.5. Federal Family Educational Rights and Privacy Act (FERPA)

2.8.6. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §3541

2.8.7. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R 164

2.8.8. United States Code, Title 18, Chapter 47, §1030: Fraud and Related Activity in Connection with Computers

2.8.9. 1 Tex. Admin. Code §202.70-76

2.8.10. Texas Government Code §556.004

2.8.11. Texas Penal Code, Chapter 33: Computer Crimes

2.8.12. Texas Penal Code, §37.10: Tampering with Governmental Record

2.8.13. TSUS Sexual Misconduct Policy and Procedures

2.8.14. LSCPA Policy 2.0 Nondiscrimination/Equal Employment Opportunity and Workforce Diversity

2.8.15. LSCPA Policy 5.0 Ethics

2.8.16. LSCPA Policy 5.1 Standards of Conduct

2.8.17. LSCPA Policy 5.2 Conflicts of Interest

2.8.18. LSCPA Policy 5.3 Fraud

2.8.19. LSCPA Policy 5.10 Use of State Property

2.8.20. LSCPA Policy 5.16 Social Media

2.8.21. LSCPA Policy 7.8 Copyright Policy

2.8.22. LSCPA Policy 9.17 Sexual Harassment

2.8.23. LSCPA Policy 11.0 Family Education Rights and Privacy Act (FERPA)

2.8.24. LSCPA Policy 11.5 Racial Harassment

2.8.25. LSCPA Information Resources Policy 1.0 Information Resources Management

2.8.26. LSCPA Information Resources Policy 6.0 Information Security Control Standards

POLICY: **3.0 ELECTRONIC AND INFORMATION RESOURCES ACCESSIBILITY**
SCOPE: **FACULTY, STAFF, AND STUDENTS**
APPROVED: **November 2007**
REVISED: **November 2020**

3.1. Policy Statement

Lamar State College Port Arthur (LSCPA) is committed to providing equal access to all users of its electronic and information resources (EIR), including persons with disabilities. Ensuring EIR are accessible is required by state and federal laws and supports the success of LSCPA's mission.

3.2. Definitions

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

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

3.3. Applicability

3.3.1. This policy applies to:

3.3.1.1. EIR developed, procured, or materially changed by LSCPA, whether by an LSCPA employee or third party acting as an agent of or on behalf of LSCPA, or through a procured services contract.

3.3.1.2. EIR services provided through hosted or managed services contracts.

3.3.1.3. EIR developed, procured, or materially changed by a contractor under a contract with LSCPA which requires the use of such product or requires the use, to a significant extent, of such product in the performance of a service or the furnishing of a product.

3.3.2. This policy does not apply to EIR that have been exempted by the Texas Department of Information Resources (DIR). A list of exempt EIR are posted under the EIR Accessibility section of the Texas DIR website.

3.4. Roles and Responsibilities

3.4.1. Institution of Higher Education President. The LSCPA President has the following responsibilities, which may be delegated:

3.4.1.1. Designate an EIR Accessibility Coordinator and inform DIR within 30 days whenever the EIR Accessibility Coordinator position is vacant or a new/replacement EIR Accessibility Coordinator is designated.

3.4.1.2. Approve exception requests for a significant difficulty or expense as described by Texas Government Code §2054.460.

3.4.1.3. Ensure appropriate staff receive training necessary to meet EIR accessibility-related requirements.

3.4.1.4. Manage an Electronic and Information Resources Accessibility Program that serves the College community in accordance with 1 Tex. Admin. Code §206 and 1 Tex. Admin. Code §213.

3.4.2. EIR Accessibility Coordinator. The EIR Accessibility Coordinator is the central point of contact concerning accessibility issues and solutions for LSCPA's EIR. The EIR Accessibility Coordinator serves in a coordinating and facilitating role, with responsibilities that include the following:

3.4.2.1. Develop, support, and maintain EIR accessibility policies, standards, and procedures.

3.4.2.2. Process EIR accessibility exception requests and maintain records of approved exceptions.

3.4.2.3. Develop and support a plan by which EIR (including websites and web applications) will be brought into compliance. The plan shall include appropriate goals, a process for corrective actions to remediate non-compliant items, and progress measurements.

3.4.2.4. Maintain documentation of accessibility testing validation procedures and results.

3.4.2.5. Facilitate a response to concerns, complaints, reported issues, and Texas DIR surveys.

3.4.2.6. Facilitate the development or acquisition of training solutions necessary to meet EIR accessibility-related requirements.

3.4.3. Unit Heads and EIR Owners

3.4.3.1. Each administrative and academic Unit Head is the default designated EIR owner for all EIR owned and/or operationally supported by the unit.

3.4.3.2. Unit Heads may designate appropriate functional leads as EIR owners.

3.4.4. EIR owners shall ensure compliance with this policy. Operational responsibility for compliance with this policy may be delegated by the EIR owner to appropriate personnel within the unit.

3.5. Procurement

3.5.1. LSCPA is required to make procurement decisions and utilize contract language that supports the acquisition of accessible EIR products and services.

3.5.2. LSCPA personnel who acquire EIR shall require vendors to provide documented accessibility information for EIR products or services. This documentation shall be retained by the procurement office. If credible accessibility documentation cannot be provided by the vendor, the product or service shall be considered noncompliant. Acceptable forms of documentation include:

3.5.2.1. Voluntary Product Accessibility Template (VPAT) or equivalent reporting template.

3.5.2.2. Credible evidence of the vendor's capability or ability to produce accessible EIR products and services. Such evidence may include, but is not limited to, a vendor's internal accessibility policy documents, contractual warranties for accessibility, accessibility testing documents, and examples of prior work results.

3.5.3. LSCPA shall monitor contracts and accessibility-related procurement processes for compliance with this policy.

3.6. Accessibility Testing and Validation

3.6.1. Accessibility testing shall be coordinated with the EIR Accessibility Coordinator.

3.6.2. New and modified web EIR shall be tested using one or more EIR accessibility validation tools to validate compliance with accessibility requirements. Tools include, but are not limited to, automated methods, manual methods, and assistive technologies.

3.6.3. Accessibility testing shall be performed and documented by a knowledgeable LSCPA employee or third party testing resource to validate compliance with 1 Tex. Admin. Code §206.70 and 1 Tex. Admin. Code §213 on all information resources technology projects for which development cost exceeds $500,000 and that meet one or more of the following criteria:

3.6.3.1. Requires one year or longer to reach operations status.

3.6.3.2. Involves more than one institution of higher education or state agency.

3.6.3.3. Substantially alters work methods or the delivery of services to clients.

3.6.4. Accessibility testing validation procedures and results shall be documented and a copy provided to the EIR Accessibility Coordinator in a timely manner.

3.7. Website and Web Application Accessibility

3.7.1. All new or modified web pages, forms, documents, and applications (web EIR) must comply with the requirements of this policy.

3.7.2. When compliance cannot be accomplished, an alternative version of the web EIR must be provided. The alternative version must have equivalent information or functionality and must be updated when the primary web EIR changes.

3.7.3. The LSCPA home page must include an Accessibility link to a web page that contains LSCPA's website accessibility policy statement (see Appendix C), site validation standard, contact information for LSCPA's web accessibility coordinator, and a link to the Governor's Committee on People with Disabilities web site.

3.7.4. LSCPA web sites shall be monitored for compliance with this policy.

3.7.4.1. College websites shall be scanned periodically (at least quarterly) using an appropriate validation tool.

3.7.4.2. Detailed validation reports shall be distributed to appropriate unit heads and EIR owners.

3.7.5. Compliance reports shall be distributed to executive management

3.8. Exceptions

3.8.1. An exception from this policy may be granted under certain circumstances, including significant difficulty or expense. Exception requests for EIR and websites that do not comply with accessibility requirements shall be submitted to the EIR Accessibility Coordinator by the unit head that owns or operationally supports the EIR. Exception requests shall contain the following information:

3.8.1.1. A date of expiration or duration of the exception.

3.8.1.2. A plan for alternate means of access for persons with disabilities.

3.8.1.3. Justification for the exception, including technical barriers, cost of remediation, fiscal impact for bringing the EIR into compliance, and other identified risks.

3.8.1.4. Documentation of how the College considered alternative solutions and all College resources available to the program or program component for which the product is being developed, procured, maintained, or used. Examples may include, but are not limited to, institution budget, grants, and alternative vendor or product selections.

3.8.2. Exception requests must be approved by the President in writing. LSCPA shall retain documentation for approved exceptions as per the appropriate records retention schedule. Documentation shall consist of the exception request and evidence that the institution of higher education considered all institution resources available to the program or program component for which the product is being developed, procured, maintained, or used.

3.9. Accessibility Standards

3.9.1. LSCPA is required to comply with EIR accessibility standards and requirements in 1 Tex. Admin. Code §206 and 1 Tex. Admin. Code §213.

3.9.2. Unless an exception has been granted, all EIR must comply with the following requirements:

3.9.2.1. Appropriate technical standards based on EIR Category (see Table 1).

3.9.2.2. Functional Performance Criteria as described in 1 Tex. Admin. Code §213.35.

3.9.2.3. Information, Documentation, and Support requirements described in 1 Tex. Admin. Code §213.36.

3.9.2.4. College guidelines and procedures published on LSCPA's IT Accessibility website.

Table 1: Technical Accessibility Standards by EIR Category

EIR Category	Technical Accessibility Standards
Software Applications & Operating Systems	1 Tex. Admin. Code §213.30
Websites	1 Tex. Admin. Code §206.70 Web Content Accessibility Guidelines (WCAG) 2.0, Level AA
Telecommunications Products	1 Tex. Admin. Code §213.31
Video and Multimedia Products	1 Tex. Admin. Code §213.32
Self-Contained, Closed Products (embedded technologies)	1 Tex. Admin. Code §213.33
Desktop and Portable Computers	1 Tex. Admin. Code §213.34

3.9.3. When compliance cannot be accomplished for an EIR, an alternative design or technology may be used provided it results in substantially equivalent or greater access for people with disabilities.

3.10. Related Policies, Regulations, Standards, and Guidelines

3.10.1. 1 Tex. Admin. Code §206.70

3.10.2. 1 Tex. Admin. Code §213

3.10.3. Texas Government Code §2054.457

3.10.4. Texas Government Code §2054.460

3.10.5. Section 508 Requirements and Standards (36 CFR, Section 1194)

3.10.6. Web Content Accessibility Guidelines (WCAG) 2.0

3.10.7. LSCPA Information Resources Policy 4.0 College Websites

POLICY: **4.0 COLLEGE WEBSITES**
SCOPE: **FACULTY AND STAFF**
APPROVED: **November 2020**
REVISED:

4.1. Policy Statements

1.1. With respect to Texas law, the Texas State University System (TSUS) Regents' Rules, and the policies of Lamar State College Port Arthur, all hardware, software, network, and data components of college websites qualify as information resources owned by Lamar State College Port Arthur.

1.2. College websites may not be used by profit-oriented third parties, or for solicitation, advertising, or other commercial purposes to the benefit of third parties, except as provided under the terms of the following regulations:

4.1.1.1. Section 39.02(a) of the Texas Penal Code prohibits the use of state property and resources for commercial purposes or personal gain.

4.1.1.2. Chapter VIII of TSUS Regents' Rules restricts the use of college facilities and equipment in solicitation, advertising and other commercial activities.

4.1.1.3. Information Resources Policy 2.0 Appropriate Use of Information Resources describes both permitted and prohibited uses of LSCPA's information resources.

4.1.2. Wherever this policy incorporates a statute, standard, or rule by reference, any definitions or descriptions provided within the referenced statute, standard or rule will prevail in the interpretation of that statute, standard, or rule.

4.2. Definitions

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

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

4.3. Applicability

4.3.1. This policy applies to all web-based content and services published on college websites that support college operations regardless of physical location. This includes college websites that are maintained by third parties.

4.3.2. Except as specified elsewhere in this policy, the provisions of this policy are generally applicable to all college websites. Unit Heads with sufficient justification may pursue exceptions using the process outlined in Section 4.8 of this policy.

4.4. Roles and Responsibilities

4.4.1. Director of Public Information

4.4.1.1. The Director of Public Information is the content owner for the college home page, which is the college's highest-level Internet web presence.

4.4.1.2. The Director of Public Information is responsible for managing the approval process for artistic design of college websites, including templates.

4.4.2. Information Technology Services

4.4.2.1. Information Technology Services is responsible for the technical design, development, maintenance, and operation of college websites that are not maintained by contracted third parties.

4.4.2.2. Information Technology Services is responsible for managing all lamarpa.edu domain names associated with college websites.

4.4.3. Unit Heads and Content Owners

4.4.3.1. Each administrative and academic Unit Head is the default designated content owner for college websites specific to their unit.

4.4.3.2. Operational responsibility for compliance with this policy may be delegated by the Unit Head to appropriate personnel within the unit.

4.4.3.3. Content Owners are responsible for maintaining content that is accurate and timely. Content should be reviewed at least yearly and be updated or deleted as necessary.

4.4.3.4. Content Owners are responsible for ensuring their content is compliant with all applicable policy, legislative, and regulatory requirements.

4.5. Design and Technical Requirements

4.5.1. College websites shall follow the branding, graphics, and design guidelines in the Lamar State College Port Arthur Brand Guide.

4.5.2. College websites designed for use by the public shall utilize approved templates.

4.5.3. All college websites and the services provided via those websites shall satisfy the standards for website accessibility in Information Resources Policy 3.0 Electronic and Information Resources Accessibility.

4.5.4. College websites should be designed to support:

4.5.4.1. variations in internet connection speeds and emerging communications protocols and technologies; and

4.5.4.2. the ability to adapt content to end user devices such as mobile phone, tablets, or other devices which are available to the general public.

4.5.5. All custom code on college websites must be reviewed and approved by Information Technology Services prior to being implemented.

4.5.6. The college home page must incorporate Texas Records and Information Locator (TRAIL) meta data as specified in 1 Tex. Admin. Code §206.74.

4.6. Linking Requirements

4.6.1. The College shall maintain a linking notice (see Appendix D) that governs the use of, copying information from, or linking to a state website that is compliant with 1 Tex. Admin. Code §206.73. The linking notice must be posted on the college home page and all key public entry points, or on the site policies page.

4.6.2. LSCPA shall ensure that college websites comply with the following linking requirements:

4.6.2.1. The college home page must include links to State of Texas resources as specified in 1 Tex. Admin. Code §206.74(b).

4.6.2.2. The college home page or site policies page must include links to college resources as specified in 1 Tex. Admin. Code §206.74(c).

4.6.2.3. The college's key public entry points must include links to college resources as specified in 1 Tex. Admin. Code §206.74(d).

4.7. Privacy

4.7.1. The college shall publish a privacy notice (see Appendix E) on the college home page and all key public entry points or on the site policies page. The privacy notice must conform to the requirements of 1 Tex. Admin. Code §206.72.

4.7.2. The college shall conduct a transaction risk assessment and implement appropriate privacy and security controls prior to:

4.7.2.1. collecting Personal Identifying Information (PII) through a college website; or

4.7.2.2. providing access to PII through a college website.

4.7.3. All web-based forms that collect information from the public must include a link to the college's website privacy notice.

4.7.4. Web-based forms that collect personal information (as defined by the Children's Online Privacy Protection Act) shall not be targeted towards children under the age of 13.

4.8. Exceptions

4.8.1. Exception requests related to accessibility shall follow the process defined in Information Resources Policy 3.0 Electronic and Information Resources Accessibility.

4.8.2. Exception requests related to information security shall follow the process defined in Information Resources Policy 5.0 Information Security Program.

4.8.3. Exception requests related to branding and artistic design shall be submitted to the Director of Public Information.

4.8.4. All other exception requests shall be submitted to the Director of Information Technology Services.

4.9. Related Policies, Regulations, Standards, and Guidelines

4.9.1. Children's Online Privacy Protection Act of 1998

4.9.2. 1 Tex. Admin. Code §206

4.9.3. 1 Tex. Admin. Code §213

4.9.4. Section 39.02(a) of the Texas Penal Code

4.9.5. Chapter VIII of TSUS Regents' Rules

4.9.6. LSCPA Information Resources Policy 1.0 Information Resources Management

4.9.7. LSCPA Information Resources Policy 2.0 Appropriate Use of Information Resources

4.9.8. LSCPA Information Resources Policy 3.0 Electronic and Information Resources Accessibility

4.9.9. LSCPA Information Resources Policy 5.0 Information Security Program

4.9.10. Lamar State College Port Arthur Brand Guide

POLICY: 5.0 INFORMATION SECURITY PROGRAM
SCOPE: FACULTY, STAFF, AND STUDENTS
APPROVED: November 2020
REVISED:

5.1. Policy Statement

5.1.1. 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 State College Port Arthur's (LSCPA) information security program.

5.1.2. 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.

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

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

5.1.5. The policy articulates a framework for LSCPA's information security program.

5.2. Definitions

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

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

5.3. Roles and Responsibilities

All members of the LSCPA community share responsibility for protecting LSCPA's information resources and, as such, are essential components of LSCPA's information security organization. Although some roles are reserved for certain positions within the College, each individual may assume one or more of 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 LSCPA information resources policies.

5.3.1. President

5.3.1.1. The President may delegate some or all the operational duties in Section 5.3.1.2 of this policy; however, the President remains ultimately responsible for the security of College information resources.

5.3.1.2. The President or designated representative must:

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

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

5.3.1.2.3. Ensure senior management support the ISO in developing required security reporting as described in Section 5.8 of this policy.

5.3.1.2.4. Ensure appropriate College personnel possess the necessary training required to assist the College in complying with information security requirements.

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

5.3.1.2.6. Annually, review and approve the College's information security program.

5.3.1.2.7. Ensure that information security management processes are part of the College's strategic planning and operational processes.

5.3.1.3. Approve exceptions to information security requirements or controls as per the exception process described in Section 5.6 of this policy.

5.3.2. Information Security Officer (ISO)

5.3.2.1. The ISO must:

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

5.3.2.1.2. 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.

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

5.3.2.1.4. Establish a security awareness training program.

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

5.3.2.1.6. Ensure annual information security risk assessments are performed and documented by information owners.

5.3.2.1.7. Review the College's inventory of information systems and related ownership and responsibilities.

5.3.2.1.8. 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.

5.3.2.1.9. 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.

5.3.2.1.10. Report, at least annually, to the President and executive management of the College the status and effectiveness of security controls.

5.3.2.1.11. Inform the IRM and the relevant information owners and custodians in the event of noncompliance with information security requirements.

5.3.2.1.12. 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.

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

5.3.3. Information Resources Manager (IRM)

5.3.3.1. The IRM is the designated default Authorizing Official for all LSCPA information systems.

5.3.4. Information Owners

5.3.4.1. LSCPA (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 LSCPA is identified in Table 2.

Table 2: Information Owners

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

5.3.4.2. Ownership responsibility for network, hardware, and software assets is assigned to the IRM by default.

5.3.4.3. Information owners must:

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

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

5.3.4.3.3. Formally assign custody and authorize the custodian to implement required security controls, if anyone other than the LSCPA Information Technology Services department is the custodian of an information resource.

5.3.4.3.4. Justify, document, and coordinate approval for exceptions as per the process described in Section 5.7 of this policy.

5.3.4.3.5. Complete risk assessments as described in Information Resources Policy 6.0 Information Security Control Standards, Section 6.13.

5.3.4.3.6. 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.

5.3.4.4. Information owners are accountable for exceptions to security requirements or controls for their information or information resources.

5.3.5. Information Custodians

5.3.5.1. The LSCPA Information Technology Services department is, by default, the custodian of all information resources for which it has system administration responsibilities. LSCPA Information Technology has the authority to implement required security controls.

5.3.5.2. Information custodians must:

5.3.5.2.1. Participate in risk assessments as described in Information Resources Policy 6.0 Information Security Control Standards, Section 6.13.

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

5.3.5.3. In consultation with the IRM and ISO, information custodians must:

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

5.3.5.3.2. Provide owners with information to facilitate the evaluation of the cost-effectiveness of controls and monitoring.

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

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

5.3.6. Users

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

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

5.3.6.3. 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.

5.3.6.4. Employee users are authorized to use only those information resources that are appropriate and consistent with their job functions and must not violate or compromise the privacy or security of any data or systems accessible via LSCPA's computer network. (See Information Resources Policy 2.0 Appropriate Use of Information Resources for additional information.)

5.4. General

5.4.1. The College must develop, document, and implement a College-wide information security program.

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

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

5.4.2. The program must:

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

5.4.2.2. Be informed by relevant federal and state legislative requirements, Texas State University System policies, regulatory requirements, and industry standards.

5.4.2.3. Contain elements that comply with relevant federal and state legislative requirements (e.g., 1 Tex. Admin. Code §202.74) and TSUS policies.

5.4.2.4. Include information security measures that inform required security reporting.

5.4.2.5. Ensure that adequate separation of duties exists for tasks that are susceptible to fraudulent activity.

5.4.2.6. Include policies, controls, standards, and procedures that:

5.4.2.6.1. Are based on risk assessments.

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

5.4.2.6.3. Ensure that information security is addressed throughout the life cycle of each institution of higher education information resource.

5.4.2.6.4. Ensure compliance with relevant federal and state legislative requirements (e.g., 1 Tex. Admin. Code §202.74), Texas State University System policies, and minimally acceptable system configuration requirements as determined by the College.

5.4.3. The ISO and IRM will implement the information security program in collaboration with all LSCPA constituents that use and support LSCPA's information resources.

5.4.4. 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.

5.4.5. Program, plan, and procedure documentation, including security-related plans identified in this and other LSCPA information resources policies, must be protected from unauthorized disclosure or modification.

5.5. Data Classification

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

5.5.1.1. Information that meets the criteria for Regulated must be assigned that classification in addition to the primary classification.

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

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

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

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

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

5.6. Information Security Risk Management

5.6.1. Risk assessments for information and information systems must be completed as per Information Resources Policy 6.0 Information Security Control Standards, Section 6.13.

5.6.2. 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.

5.6.3. The ISO will commission periodic reviews of LSCPA'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.

5.7. Information Security Exceptions

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

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

5.7.3. Requests must contain the following information:

5.7.3.1. The policy for which the exception is sought.

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

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

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

5.7.3.5. Risk management rationale.

5.7.4. 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 and the approval of the LSCPA President and executive management.

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

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

5.7.7. Approved security exceptions must be included in LSCPA's risk assessment process.

5.8. Information Security Reporting

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

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

5.8.1.2. Compliance with information security requirements.

5.8.1.3. Residual risks identified by the College's risk management process.

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

5.8.1.5. The College's information security requirements and requests such as security exceptions and requests for resources.

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

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

5.8.3.1. 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 Information Resources Policy 6.0 Information Security Control Standards, Section 6.9.5.)

5.9. Related Policies, Regulations, Standards, and Guidelines

5.9.1. 1 Tex. Admin. Code §202.70

5.9.2. 1 Tex. Admin. Code §202.71

5.9.3. 1 Tex. Admin. Code §202.72

5.9.4. 1 Tex. Admin. Code §202.73

5.9.5. 1 Tex. Admin. Code §202.74

5.9.6. 1 Tex. Admin. Code §202.75

5.9.7. Texas Government Code §2054.133

5.9.8. LSCPA Information Resources Policy 1.0 Information Resources Management

5.9.9. LSCPA Information Resources Policy 6.0 Information Security Control Standards

POLICY: 6.0 INFORMATION SECURITY CONTROL STANDARDS
SCOPE: FACULTY, STAFF, AND STUDENTS
APPROVED: November 2020
REVISED: April 2024

6.1. Policy Statement

6.1.1. Purpose: The purpose of this policy is to define information security control standards for Lamar State College Port Arthur (LSCPA) information systems and data, guided by required elements of the Texas Department of Information Resources Security Control Standards Catalog.

6.1.2. Scope: This policy applies to the Lamar State College Port Arthur (LSCPA). All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the college's information resources.

6.1.3. Application: The statements in this document establish the requirements for Lamar State College Port Arthur. At the discretion of the college, more stringent, restrictive, or enhanced requirements may be established.

6.1.4. Management: This policy is managed by the Lamar State College Chief Information Security Officer and will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate college personnel.

6.2. Definitions

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

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

6.3. Access Control

6.3.1. Procedures (Authority - DIR Controls Catalog (CC): AC-1)

6.3.1.1. LSCPA must:

6.3.1.1.1. Develop procedures to facilitate the implementation of the Access Control policy and associated access controls;

6.3.1.1.2. Review and update Access Control procedures at a college defined frequency; and

6.3.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Access Control procedures related to the controls in this policy.

6.3.2. Account Management & Disable Accounts (Authority - DIR CC: AC-2, AC-2(3), TAC 202.72)

6.3.2.1. Define and document, in consultation with the college's ISO and IRM, the types of information system accounts that support organizational missions and business functions.

6.3.2.2. Assign account manager responsibilities for information system accounts to the respective information owner.

6.3.2.3. Establish conditions for group and role membership.

6.3.2.4. Require the respective information owner to specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

6.3.2.5. Require approval from the information owner for requests to create information system accounts.

6.3.2.6. Require the respective information custodian to create, enable, modify, disable, and remove information system accounts in accordance with college-defined procedures and conditions.

6.3.2.7. Require the respective information custodian to monitor the use of information system accounts.

6.3.2.8. Notify account managers (i.e., information owners) within a college-defined period of time for each of the following conditions:

6.3.2.8.1. when the accounts are no longer required;

6.3.2.8.2. when users are terminated or transferred; and

6.3.2.8.3. when individual information system usage or need-to-know changes.

6.3.2.9. Require that determinations to authorize access to each information system by the respective information owner are based on:

6.3.2.9.1. a valid access authorization request;

6.3.2.9.2. intended system usage; and

6.3.2.9.3. other attributes as required by mission or business functions.

6.3.2.10. Require respective information custodians to review accounts for compliance with account management requirements at least once every two years or more frequently as defined by LSCPA.

6.3.2.11. Require respective information owners and information custodians to establish and implement processes for changing shared/group account credentials (if deployed) when individuals are removed from a group.

6.3.2.12. Align account management processes with personnel termination and transfer processes.

6.3.2.13. Disable accounts within a college-defined period of time when the accounts:

6.3.2.13.1. Have expired,

6.3.2.13.2. Are no longer associated with a user or individual,

6.3.2.13.3. Are in violation of college policy, or

6.3.2.13.4. Have been inactive for a college-defined period of time.

6.3.3. Access Enforcement (Authority - DIR CC: AC-3)

6.3.3.1. LSCPA must ensure that information systems enforce approved authorizations for logical access to information and system resources in accordance with applicable, college-defined access control policies.

6.3.4. Separation of Duties (Authority - DIR CC: AC-5)

6.3.4.1. LSCPA must:

6.3.4.1.1. Identify and document separation of duties of individuals based on college-defined criteria; and

6.3.4.1.2. Require that information owners define information system access authorizations to support separation of duties.

6.3.5. Least Privilege (Authority - DIR CC: AC-6)

6.3.5.1. LSCPA must:

6.3.5.1.1. Establish the principle of least privilege as a critical and strategic component of college-level information security policies and procedures; and

6.3.5.1.2. Ensure that access to information systems for users and processes acting on behalf of users is based on the principle of least privilege..

6.3.6. Unsuccessful Logon Attempts (Authority - DIR CC: AC-7).

6.3.6.1. LSCPA must ensure that each information system:

6.3.6.1.1. Enforces a college-defined limit of consecutive, invalid logon attempts by a user or source of authentication during a college-defined period of time; and

6.3.6.1.2. Automatically performs at least one of the following actions when the maximum number of unsuccessful attempts is exceeded:

- Locks the account or node for a college-defined period of time;
- Locks the account or node until released by an administrator;
- Delays the next logon prompt according to a college-defined delay algorithm; and/or

6.3.6.1.3. Notifies the information custodian.

6.3.7. System Use Notification (Authority - DIR CC: AC-8)

6.3.7.1. LSCPA must ensure that each information system:

6.3.7.1.1. Displays to human users at logon interfaces a college-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

- Users are accessing a college information system;
- Information system usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the information system is prohibited and subject to criminal prosecution and civil penalties; and

- Use of the information system indicates consent to monitoring and recording;

6.3.7.1.2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to logon to or further access the information system; and

6.3.7.1.3. For publicly accessible systems that do not have logon interfaces:

- Displays system use information under college-defined conditions before granting further access.
- Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- Includes a description of the authorized uses of the system.

6.3.8. Permitted Actions Without Identification or Authentication (Authority - DIR CC: AC-14)

6.3.8.1. LSCPA must:

6.3.8.1.1. Identify and define user actions that can be performed on college information systems without identification or authentication consistent with college missions and business functions; and

6.3.8.1.2. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication .

6.3.9. Remote Access (Authority - DIR CC: AC-17)

6.3.9.1. LSCPA must:

6.3.9.1.1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

6.3.9.1.2. Authorize each type of remote access to each information system prior to allowing such connections..

6.3.10. Wireless Access (Authority - DIR CC: AC-18)

6.3.10.1. LSCPA must:

6.3.10.1.1. Establish configuration and connection requirements, and implementation guidance for each type of wireless access; and

6.3.10.1.2. Authorize each type of wireless access to each information system prior to allowing such connections.

6.3.11. Access Control for Mobile Devices (Authority - DIR CC: AC-19)

6.3.11.1. LSCPA must:

6.3.11.1.1. Establish configuration requirements, connection requirements, and implementation guidance for college-controlled mobile devices, to include when such devices are outside of college-controlled networks; and

6.3.11.1.2. Authorize the connection of mobile devices to college information systems.

6.3.12. Use of External Systems (Authority - DIR CC: AC-20)

6.3.12.1. LSCPA must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

6.3.12.1.1. Access the information system from external information systems; and

6.3.12.1.2. Process, store, or transmit college-controlled information using external information systems.

6.3.13. Publicly Accessible Content (Authority- DIR CC: AC-22)

6.3.13.1. LSCPA must:

6.3.13.1.1. Designate individuals authorized to make information publicly accessible;

6.3.13.1.2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

6.3.13.1.3. Review the proposed content of information prior to posting onto publicly accessible information systems to ensure that nonpublic information is not included; and

6.3.13.1.4. Review the content on the publicly accessible information system for nonpublic information at college defined frequencies and remove such information, if discovered.

6.4. Awareness and Training

6.4.1. Procedures (Authority - DIR CC: AT-1, TGC 2054.519, TGC 5054.5191, TGC 2054.5192)

6.4.1.1. LSCPA must:

6.4.1.1.1. Develop procedures to facilitate the implementation of the Awareness and Training policy and associated controls;

6.4.1.1.2. Review and update Awareness and Training procedures at a college-defined frequency; and

6.4.1.1.3. Designate a college employee as responsible for managing, developing, documenting, and disseminating college Awareness and Training procedures related to the controls in this policy; and

6.4.1.1.4. Provide information security training for all users of college information systems in accordance with applicable state and federal law, including, but not limited to, Texas Government Code § 2054.519, §2054.5191, and §2054.5192.

6.4.2. Literacy Training and Awareness & Insider Threat (Authority - DIR CC: AT-2, AT-2(2), TGC 2054.519, TGC 2054.5191, TGC 2054.5192)

6.4.2.1. LSCPA must:

6.4.2.1.1. Provide security literacy training to:

- Employees at least annually or as required by changes to information systems;
- New employees during the onboarding process; and
- Contractors who have access to a component institution's computer system or database.

6.4.2.1.2. Update security awareness and literacy training at an institution-defined frequency; and

6.4.2.1.3. Provide literacy training on recognizing and reporting potential indicators of insider threat

6.4.3. Role-Based Training (Authority - DIR CC: AT-3, TGC 2054.519, TGC 2054.5191, TGC 2054.5192)

6.4.3.1. LSCPA must:

6.4.3.1.1. Provide role-based security training:

- To information resource employees with administrative privileges and responsibilities;
- Before authorizing access to information systems, information, or performing assigned duties;
- To information resource employees on a recurring basis (at least annually) and when required by system changes.

6.4.3.1.2. Update role-based training content at a college-defined frequency.

6.4.4. Training Records (Authority - DIR CC: AT-4, TGC 2054.519, TGC 2054.5191, TGC 2054.5192)

6.4.4.1. LSCPA must:

6.4.4.1.1. Document and monitor information security training activities, including security awareness training and specific role-based security training; and

6.4.4.1.2. Retain individual training records for a college-defined time period.

6.5. Audit and Accountability

6.5.1. Procedures (Authority - DIR CC: AU-1)

6.5.1.1. LSCPA must:

6.5.1.1.1. Develop procedures to facilitate the implementation of the Audit and Accountability policy and associated controls;

6.5.1.1.2. Review and update Audit and Accountability procedures at a college-defined frequency; and

6.5.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college

Audit and Accountability procedures related to the controls in this policy.

6.5.2. Event Logging (Authority - DIR CC: AU-2)

6.5.2.1. LSCPA must:

6.5.2.1.1. Document a standard defining the types of events that each information system shall log, including the frequency at which the types of events selected for logging are reviewed and updated;

6.5.2.1.2. Identify, for each information system, the types of events that the system is capable of logging in support of the audit function as specified in the college's Standard;

6.5.2.1.3. Require information owners and information custodians to coordinate with the college's ISO (or their designee) to coordinate event logging functions;

6.5.2.1.4. Specify the types of events from its standard that are configured for logging within each information system along with the frequency of (or situation requiring) logging for each identified type of event;

6.5.2.1.5. Provide a rationale for why the college-defined auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

6.5.2.1.6. Review and update event types selected for logging according to the Standard for each information system.

6.5.2.2. LSCPA must:

6.5.2.2.1. Ensure information systems provide the means whereby authorized personnel have the ability to audit and establish individual accountability for each action that can potentially cause access to, generation or modification of, or affect the release of confidential information;

6.5.2.2.2. Ensure appropriate audit trails are maintained to provide accountability for updates to mission-critical information, hardware and software, and for all changes to automated security or access rules; and

6.5.2.2.3. Based upon an assessment of risk, maintain a sufficiently complete history of transactions to permit an audit of the information system by logging and tracing the activities of individuals through each information system

6.5.3. Content of Audit Records (Authority - DIR CC: AU-3)

6.5.3.1. LSCPA must ensure that each information system's audit records contain the following information:

6.5.3.1.1. What type of event occurred;

6.5.3.1.2. When the event occurred;

6.5.3.1.3. Where the event occurred;

6.5.3.1.4. Source of the event;

6.5.3.1.5. Outcome of the event; and

6.5.3.1.6. Identity of any individuals, subjects, or objects/entities associated with the event.

6.5.3.2. Events should contain all information needed to determine the logical location of the user.

6.5.4. Audit Log Storage Capacity (Authority - DIR CC: AU-4)

6.5.4.1. LSCPA must:

6.5.4.1.1. Allocate audit-log storage capacity to accommodate the college’s audit log retention requirements .

6.5.5. Response to Audit Logging Process Failures (Authority - DIR CC: AU-5)

6.5.5.1. LSCPA must:

6.5.5.1.1. Document in a standard the audit processing failures that generate alerts, the appropriate personnel or roles to alert, the time period in which to be alerted, and any additional actions to take;

6.5.5.1.2. In accordance with the standard, configure information systems to send designated alerts to appropriate personnel or roles in the event of applicable audit processing failures; and

6.5.5.1.3. Take any additional actions in accordance with the standard in the event of an audit logging process failure of an information system.

6.5.6. Audit Review, Analysis, and Reporting (Authority - DIR CC: AU-6)

6.5.6.1. LSCPA must:

6.5.6.1.1. Document in a standard the frequency at which information system audit records are reviewed and analyzed;

6.5.6.1.2. Review and analyze information system audit records in accordance with the frequency specified in the standard and report actionable findings to the appropriate information system custodians; and

6.5.6.1.3. Adjust the level of audit record review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

6.5.7. Time Stamps (Authority - DIR CC: AU-8)

6.5.7.1. LSCPA must:

6.5.7.1.1. Configure each information system to:

- Use internal system clocks to generate time stamps for audit records; and
- Synchronize internal system clocks with an authoritative source of time specified by the ISO and IRM;

6.5.7.1.2. Ensure that audit records record time stamps in milliseconds and:

- Use Coordinated Universal Time;
- Have a fixed local time offset from Coordinated Universal Time; or
- Include the local time offset as part of the timestamp.

6.5.8. Protection of Audit Information (Authority - DIR CC: AU-9)

6.5.8.1. LSCPA must protect audit information and audit tools from unauthorized access, modification, and deletion .

6.5.9. Audit Record Retention (Authority - DIR CC: AU-11)

6.5.9.1. LSCPA must:

6.5.9.1.1. Ensure records retention policies for audit records meets regulatory and college information retention requirements; and

6.5.9.1.2. Retain audit records for a period no less than is required by its records retention policy to provide sufficient support for after-the-fact investigations of security incidents.

6.5.10. Audit Record Generation (Authority - DIR CC: AU-12)

6.5.10.1. LSCPA must ensure that information systems:

6.5.10.1.1. Provide audit record generation capability for the auditable events required by this policy and related college policies and standards;

6.5.10.1.2. Allow authorized personnel or roles to select which auditable events are to be audited by specific components of the information system; and

6.5.10.1.3. In alignment with this policy and related college policies and standards, generate audit records for necessary types of events and ensure the generated records contain sufficient content.

6.6. Assessment, Authorization and Monitoring Policy

6.6.1. Procedures (Authority - DIR CC: CA-1)

6.6.1.1. LSCPA must:

6.6.1.1.1. Develop procedures to facilitate the implementation of the Security Assessment, Authorization, and Monitoring policy and associated controls;

6.6.1.1.2. Review and update Security Assessment, Authorization, and Monitoring procedures at a college-defined frequency; and

6.6.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Assessment, Authorization, and Monitoring procedures related to the controls in this policy.

6.6.2. Control Assessments (Authority - DIR CC: CA-2)

6.6.2.1. LSCPA must:

6.6.2.1.1. Develop a control assessment plan that describes the scope of the assessment including:

- Controls and control enhancements under assessment;
- Assessment procedures to be used to determine control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

6.6.2.1.2. Ensure the control assessment plan is reviewed and approved by the authorizing official or the authorizing official's designated representative prior to conducting the assessment;

6.6.2.1.3. Assess the controls in the information system and its environment of operation on a recurring frequency established by the college's ISO 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;

6.6.2.1.4. Produce a control assessment report that documents the results of the assessment; and

6.6.2.1.5. Provide the results of the control assessment to appropriate personnel including information owners and information custodians.

6.6.2.2. LSCPA must ensure that a review of the college's information security program for compliance with security standards set by the Texas Department of Information Resources is performed at least biennially, based on college risk management decisions. The review must be performed by individual(s) independent of the college's information security program and designated by the college's head or their designated representative(s).

6.6.3. Information Exchange (Authority - DIR CC: CA-3)

6.6.3.1. LSCPA must:

6.6.3.1.1. Through relevant information system owners, authorize the exchange of information (i.e., interconnections) between college information systems and other information systems, including those external to the college;

6.6.3.1.2. Use a formalized Interconnection Security Agreement to document interconnections. At minimum, Interconnection Security Agreements must include the following information for each information system:

- Interface characteristics;
- Security requirements, controls, and responsibilities;
- Information system category; and
- The nature of the information communicated, including data classification.

6.6.3.2. Regularly review and update as necessary established Interconnection Security Agreements at the time of periodic risk assessments or at a college-defined frequency.

6.6.4. Plan of Action and Milestones (Authority - DIR CC: CA-5)

6.6.4.1. LSCPA must:

6.6.4.1.1. Develop a Plan of Action and Milestones for each information system to document the college's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls relevant to an information system and to reduce or eliminate known vulnerabilities in the assessed system; and

6.6.4.1.2. Update existing plans of action and milestones at a college-defined frequency based on the findings from controls assessments, audits, and continuous monitoring activities.

6.6.5. Authorization (Authority - DIR CC: CA-6)

6.6.5.1. LSCPA must:

6.6.5.1.1. Assign a senior-level executive or manager as the Authorizing Official for each information system;

6.6.5.1.2. Assign a senior-level executive or manager as the Authorizing Official for common controls available for inheritance by college information systems;

6.6.5.1.3. Ensure that the Authorizing Official for an information system accepts the use of common controls inherited by the system and authorizes the information system for processing before commencing operations;

6.6.5.1.4. Ensure that the Authorizing Official for common controls authorizes the use of those controls for inheritance by college information systems; and

6.6.5.1.5. Update the security authorization at the time of periodic risk assessment for the information system or at a college-defined frequency.

6.6.6. Continuous Monitoring & Risk Monitoring (Authority - DIR CC: CA-7, CA-7(4))

6.6.6.1. LSCPA must develop a continuous monitoring strategy and implement an information system-level continuous monitoring program that includes:

6.6.6.1.1. Establishment of system-level metrics to be monitored;

6.6.6.1.2. Establishment of frequencies for monitoring and for control assessments supporting such monitoring;

6.6.6.1.3. Ongoing control assessments in accordance with the college continuous monitoring strategy;

6.6.6.1.4. Ongoing monitoring of information system and college-defined metrics in accordance with the college continuous monitoring strategy;

6.6.6.1.5. Correlation and analysis of security-related information generated by control assessments and monitoring;

6.6.6.1.6. Response actions to address results of the analysis of control assessment and monitoring information; and

6.6.6.1.7. Reporting the security status of each information system to appropriate stakeholders at a college-defined frequency.

6.6.6.2. LSCPA must ensure that risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

6.6.6.2.1. Effectiveness monitoring;

6.6.6.2.2. Compliance monitoring; and

6.6.6.2.3. Change monitoring.

6.6.7. Penetration Testing (Authority - DIR CC: CA-8; TGS §2054.516(a)(2))

6.6.7.1. LSCPA must conduct penetration testing at a college-defined frequency on college-defined information systems and information system components.

6.6.7.2. LSCPA must ensure that:

6.6.7.2.1. Internet websites or mobile applications that process any sensitive personal information, personally identifiable information, or confidential information are subjected to a vulnerability and penetration test at a college-defined frequency; and

6.6.7.2.2. Ensure that any vulnerability identified in each test is addressed in a fashion commensurate to the risks presented as determined by the college's ISO (or designee).

6.6.8. Internal System Connections (Authority - DIR CC: CA-9)

6.6.8.1. LSCPA must:

6.6.8.1.1. Authorize internal connections of college-defined information system components or classes of components to each information system;

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

6.6.8.1.3. Terminate internal system connections based on college-defined conditions; and

6.6.8.1.4. Review the need for each internal connection at a college-defined frequency.

6.7. Configuration Management

6.7.1. Procedures (Authority - DIR CC: CM-1)

6.7.1.1. LSCPA must:

6.7.1.1.1. Develop procedures to facilitate the implementation of the Configuration Management policy and associated controls;

6.7.1.1.2. Review and update Configuration Management procedures at a college-defined frequency; and

6.7.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Configuration Management procedures related to the controls in this policy.

6.7.2. Baseline Configuration (Authority - DIR CC: CM-2)

6.7.2.1. LSCPA must:

6.7.2.1.1. Develop, document, and maintain under configuration control, a current baseline configuration of each information system; and

6.7.2.1.2. Review and update the baseline configuration of each information system:

- At a college-defined frequency;
- When required because of college-defined circumstances; and
- When information system components are installed or upgraded.

6.7.3. Configuration Change Control (Authority - DIR CC: CM- 3

6.7.3.1. LSCPA must:

6.7.3.1.1. Determine and document the types of changes to information systems that are configuration-controlled;

6.7.3.1.2. Review proposed configuration-controlled changes to information systems and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

6.7.3.1.3. Document configuration change decisions associated with the information systems;

6.7.3.1.4. Implement approved configuration-controlled changes to the information systems;

6.7.3.1.5. Retain records of configuration-controlled changes to information systems for an institution-defined period of time;

6.7.3.1.6. Monitor and review activities associated with configuration-controlled changes to information systems; and

6.7.3.1.7. Coordinate and provide oversight for configuration change control activities through college-defined configuration change control elements that convenes at a college-defined frequency and/or when college-denied configuration change conditions are met.

6.7.3.2. LSCPA must ensure that all security-related information resources changes are approved by the information owner (or designee) through a change control process.

6.7.4. Impact Analyses (Authority - DIR CC: CM- 4)

6.7.4.1. LSCPA must analyze changes to each information system to determine potential security impacts prior to change implementation.

6.7.4.2. LSCPA must ensure that:

6.7.4.2.1. All security-related information resources changes are approved by the information owner (or designee) through a change control process; and

6.7.4.2.2. Such approval occurs prior to implementation by the college or independent contractors.

6.7.5. Access Restrictions for Change (Authority - DIR CC: CM- 5)

6.7.5.1. LSCPA must define, document, approve, and enforce physical and logical access restrictions associated with changes to each information system.

6.7.6. Configuration Settings (Authority - DIR CC: CM- 6)

6.7.6.1. LSCPA must:

6.7.6.1.1. Establish and document configuration settings for components employed within information systems using college-defined, common security configurations that reflect the most restrictive mode consistent with operational requirements;

6.7.6.1.2. Implement the configuration settings;

6.7.6.1.3. Identify, document, and approve any deviations from established configuration settings for college-defined information system components based on college-defined operational requirements; and

6.7.6.1.4. Monitor and control changes to the configuration settings in accordance with college policies and procedures.

6.7.7. Least Functionality (Authority - DIR CC: CM- 7)

6.7.7.1. LSCPA must:

6.7.7.1.1. Configure each information system to provide only college-defined, mission-essential capabilities; and

6.7.7.1.2. Prohibit or restrict the use of college-defined functions, ports, protocols, software and/or services.

6.7.8. System Component Inventory (Authority - DIR CC: CM- 8)

6.7.8.1. LSCPA must:

6.7.8.1.1. Develop and document an inventory of information system components that:

- Accurately reflects the information system;
- Includes all components within each information system;
- Is at the level of granularity deemed necessary for tracking and reporting;

- Includes college-defined information deemed necessary to achieve effective information system component accountability; and

6.7.8.1.2. Review and update the information system component inventory at a college-defined frequency.

6.7.9. Software Usage Restrictions (Authority - DIR CC: CM- 10)

6.7.9.1. LSCPA must:

6.7.9.1.1. Use software and associated documentation in accordance with contract agreements and copyright laws;

6.7.9.1.2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

6.7.9.1.3. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

6.7.10. User-Installed Software (Authority - DIR CC: CM- 11)

6.7.10.1. LSCPA must:

6.7.10.1.1. Establish college-defined policies governing the installation of software by users;

6.7.10.1.2. Enforce software installation policies through college-defined methods; and

6.7.10.1.3. Monitor policy compliance at college-defined frequency.

6.8. Contingency Planning

6.8.1. Procedures (Authority -DIR CC: CP-1)

6.8.1.1. LSCPA must:

6.8.1.1.1. Develop procedures to facilitate the implementation of the Contingency Planning policy and associated controls;

6.8.1.1.2. Review and update Contingency Planning procedures at a college-defined frequency;

6.8.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Contingency Planning procedures related to the controls in this policy; and

6.8.1.1.4. Maintain written continuity of operations plans that address information resources.

6.8.2. Contingency Plan (Authority - DIR CC: CP-2)

6.8.2.1. LSCPA must:

6.8.2.1.1. Develop a contingency plan for each information system that:

- Identifies essential missions and business functions and associated contingency requirements;
- Provides recovery objectives, restoration priorities, and metrics;
- Addresses contingency roles, responsibilities, and assigned individuals with contact information;
- Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- Addresses eventual, full information system restoration without deterioration of the controls originally planned and implemented; and
- Is reviewed and approved by college designated personnel or roles;

6.8.2.1.2. Distribute copies of the contingency plan to college designated key contingency personnel (identified by name and/or by role) and college elements;

6.8.2.1.3. Coordinate contingency planning activities with incident handling activities;

6.8.2.1.4. Review the contingency plan for each information system at a college-defined frequency;

6.8.2.1.5. Update the contingency plan to address changes to the college, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

6.8.2.1.6. Communicate contingency plan changes to college designated key contingency personnel (identified by name and/or by role) and college elements; and

6.8.2.1.7. Protect the contingency plan from unauthorized disclosure and modification.

6.8.3. Contingency Training (Authority - DIR CC: CP-3)

6.8.3.1. LSCPA must provide contingency training to information system users consistent with assigned roles and responsibilities:

6.8.3.1.1. Within a college-defined time period of assuming a contingency role or responsibility;

6.8.3.1.2. When required by information system changes; and

6.8.3.1.3. On a college-defined frequency thereafter.

6.8.4. Contingency Plan Testing (Authority - DIR CC: CP-4)

6.8.4.1. LSCPA must:

6.8.4.1.1. Test the contingency plan for information systems at least annually using college-defined tests to determine the effectiveness of the plan and the college readiness to execute the plan;

6.8.4.1.2. Review the contingency plan test results; and

6.8.4.1.3. Initiate corrective actions, if needed.

6.8.5. Alternate Storage Site (Authority - DIR CC: CP-6)

6.8.5.1. LSCPA must:

6.8.5.1.1. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information; and

6.8.5.1.2. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

6.8.6. Telecommunications Services (Authority - DIR CC: CP-8)

6.8.6.1. LSCPA must establish alternate telecommunications services, including necessary agreements to permit the resumption of college-defined information system operations for essential mission and business functions within an college-defined period of time when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

6.8.7. System Backup (Authority - DIR CC: CP-9)

6.8.7.1. LSCPA must:

6.8.7.1.1. Conduct backups of the following types of information at a frequency consistent with college-defined recovery time and recovery point objectives:

- User-level information contained in information systems;
- System-level information contained in information systems; and
- Information system documentation, including security-related documentation;

6.8.7.1.2. Protect the confidentiality, integrity, and availability of backup information.

6.8.8. System Recovery and Reconstitution (Authority - DIR CC: CP-10)

6.8.8.1. LSCPA must have the capability for recovery and reconstitution of each information system to a known state after a disruption, compromise, or failure consistent with college-defined recovery time and recovery point objectives.

6.8.9. Alternate Communications Protocols (Authority - DIR CC: CP-11)

6.8.9.1. LSCPA must have the capability to employ college-defined alternative communications protocols in support of maintaining continuity of operations.

6.9. Identification and Authentication

6.9.1. Procedures (Authority - DIR CC: IA-1)

6.9.1.1. LSCPA must:

6.9.1.1.1. Develop procedures to facilitate the implementation of the Identification and Authentication policy and associated controls;

6.9.1.1.2. Review and update Identification and Authentication procedures at a college-defined frequency; and

6.9.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Identification and Authentication procedures related to the controls in this policy.

6.9.2. Identification and Authentication (Organizational Users), Multifactor Authentication to Privileged Accounts, & Multifactor Authentication to Non-privileged Accounts (Authority - DIR CC: IA-2, IA-2(1), IA-2(2); TAC 202.1)

6.9.2.1. LSCPA must ensure that information systems uniquely identify and authenticate college users or processes acting on behalf of college users prior to granting the user or process access to a given information system.

6.9.2.1.1. Non-unique identifiers may only be used in situations in which risk analysis performed by college-defined personnel demonstrates no need for individual accountability of users.

6.9.2.2. LSCPA must implement multifactor authentication for access to privileged accounts on college information systems.

6.9.2.3. LSCPA must implement multifactor authentication for access to non-privileged accounts on college information systems.

6.9.3. Identifier Management (Authority - DIR CC: IA-4)

6.9.3.1. LSCPA must manage information system identifiers by:

6.9.3.1.1. Receiving authorization from college-defined personnel to assign an individual, group, role, service, or device identifier;

6.9.3.1.2. Selecting an identifier that identifies an individual, group, role, service, or device;

6.9.3.1.3. Assigning the identifier to the intended individual, group, role, service, or device; and

6.9.3.1.4. Preventing reuse of identifiers for a college-defined time period.

6.9.3.2. LSCPA must ensure a user’s access authorization is appropriately modified or removed when the user’s employment, job responsibilities, or affiliation with the college changes.

6.9.4. Authenticator Management (Authority - DIR CC: IA-5)

6.9.4.1. LSCPA must manage information system authenticators by:

6.9.4.1.1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

6.9.4.1.2. Establishing initial authenticator content for authenticators defined by the college;

6.9.4.1.3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

6.9.4.1.4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

6.9.4.1.5. Changing default authenticators prior to first use;

6.9.4.1.6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

6.9.4.1.7. Changing or refreshing authenticators at a college-defined time period by authenticator type;

6.9.4.1.8. Protecting authenticator content from unauthorized disclosure and modification;

6.9.4.1.9. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and

6.9.4.1.10. Changing authenticators for group or role accounts when membership to those accounts changes.

6.9.5. Password-based Authentication (Authority - DIR CC: IA-5(1))

6.9.5.1. For password-based authentication, LSCPA must:

6.9.5.1.1. Maintain a list of commonly used, expected, or compromised passwords and update the list at a college-defined frequency and when college passwords are suspected to have been compromised directly or indirectly;

6.9.5.1.2. Verify, when users create or update passwords, that the passwords are not found on the college-defined list of commonly used, expected, or compromised passwords;

6.9.5.1.3. Transmit passwords only over cryptographically protected channels;

6.9.5.1.4. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

6.9.5.1.5. Require immediate selection of a new password upon account recovery;

6.9.5.1.6. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

6.9.5.1.7. Employ automated tools to assist the user in selecting strong password authenticators; and

6.9.5.1.8. Enforce college-defined password composition and complexity rules.

6.9.6. Authenticator Feedback (Authority - DIR CC: IA-6)

6.9.6.1. LSCPA must ensure that information systems obscure feedback of authentication information entered during authentication processes.

6.9.7. Cryptographic Module Authentication (Authority - DIR CC: IA-7)

6.9.7.1. LSCPA must:

6.9.7.1.1. Implement mechanisms for authentication to cryptographic modules in information systems; and

6.9.7.1.2. Ensure that implemented cryptographic modules meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

6.9.8. Identification and Authentication (Non-Organizational Users) (Authority - DIR CC: IA-8)

6.9.8.1. LSCPA must ensure that information systems uniquely identify and authenticate non-college users or processes acting on behalf of non-college users.

6.9.9. Re-Authentication (Authority - DIR CC: IA-11)

6.9.9.1. LSCPA must document a Standard defining the circumstances or situations which require users to re-authenticate.

6.9.9.2. LSCPA must require users to re-authenticate according to the component college's Standard.

6.9.9.3. LSCPA's standard for re-authentication must include the following minimum requirements:

6.9.9.3.1. Users must be required to re-authenticate when a device automatically locks; and

6.9.9.3.2. Users must be required to re-authenticate when the user's password is known to be compromised or publicly disclosed.

6.10. Incident Response

6.10.1. Procedures (Authority - DIR CC: IR-1)

6.10.1.1. LSCPA must:

6.10.1.1.1. Develop procedures to facilitate the implementation of the Incident Response policy and associated controls; and

6.10.1.1.2. Review and update Incident Response procedures at a college-defined frequency; and

6.10.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Incident Response procedures related to the controls in this policy.

6.10.1.2. LSCPA must assess the significance of a security incident based upon the business impact on the affected resources and the current and potential technical effect of the incident.

6.10.2. Incident Response Training (Authority - DIR CC: IR-2)

6.10.2.1. LSCPA must provide incident response training to information system users consistent with their assigned roles and responsibilities:

6.10.2.1.1. Within a college-defined time period of assuming an incident response role or responsibility or acquiring information system access;

6.10.2.1.2. When required by information system changes; and

6.10.2.1.3. At an annual frequency thereafter.

6.10.3. Incident Response Testing (Authority - DIR CC: IR-3)

6.10.3.1. LSCPA must test the effectiveness of the incident response capability for each information system at a college-defined frequency using the college-defined tests for each information system.

6.10.4. Incident Handling (Authority - Texas Administrative Code (TAC): 202.73(b); DIR CC: IR-4)

6.10.4.1. LSCPA must:

6.10.4.1.1. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery

6.10.4.1.2. Coordinate incident handling activities with contingency planning activities;

6.10.4.1.3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

6.10.4.1.4. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the college.

6.10.5. Incident Monitoring (Authority - TAC 202.73(b); DIR CC: IR-5)

6.10.5.1. LSCPA must track and document security and supply chain incidents.

6.10.6. Incident Reporting (Authority - TAC 202.73(b); DIR CC: IR-6)

6.10.6.1. LSCPA must:

6.10.6.1.1. Require personnel to report suspected security and supply chain incidents to the college’s ISO (or their designee) using college-defined procedures within a college-defined time period;

6.10.6.1.2. Develop policies and mechanisms providing for notification to the ISO (or their designee) any Suspected Data Breach within 48 hours of discovery;

6.10.6.1.3. Promptly report security and supply chain incidents to the Department of Information Resources (DIR) when the security incident is assessed to:

- Propagate to other state information systems;
- Result in criminal violations that shall be reported to law enforcement in accordance with state or federal information security or privacy laws;
- Involve the unauthorized disclosure or modification of confidential information; or
- be an unauthorized incident that compromises, destroys, or alters information systems, applications, or access to such systems or applications in any way.

6.10.6.1.4. Report summary security and supply chain incident information monthly to DIR no later than 9 calendar days after the end of the month.

6.10.6.2. If an information security or supply chain incident is required to be reported to the DIR under Texas Government Code Sec. 2054.1125 or the "Urgent Incident Report" rules per Texas Administrative Code 202.73(b), the college's established reporting and escalation procedures shall also require notification to the Texas State University System Administration via the Vice Chancellor and Chief Financial Officer and the Chief Audit Executive in a similar reporting manner and timeline.

6.10.7. Incident Response Assistance (Authority - DIR CC: IR-7)

6.10.7.1. LSCPA must provide an incident response resource, integral to the college's incident response capability, that advises and assists users of information systems in handling and reporting security and supply chain incidents. The incident response resource must be determined by the college's ISO and may be comprised of technical support personnel, verified third-party consultants, and other resources.

6.10.8. Incident Response Plan (Authority - DIR CC: IR-8)

6.10.8.1. LSCPA must:

6.10.8.1.1. Develop an incident response plan that:

- Provides the college with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits in to the overall college;
- Meets the unique requirements of the college, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the college;
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by appropriate, college-defined leadership; and
- Explicitly designates responsibility for incident response to college-defined roles.

6.10.8.2. Distribute copies of the incident response plan to college elements charged with incident response responsibilities defined by name and/or role;

6.10.8.3. Update the incident response plan to address system and college changes or problems encountered during plan implementation, execution, or testing;

6.10.8.4. Communicate changes to the incident response plan to college elements charged with incident response responsibilities defined by name and/or role; and

6.10.8.5. Protect the incident response plan from unauthorized disclosure and modification.

6.10.9. Information Spillage Response (Authority - DIR CC: IR-9)

6.10.9.1. LSCPA must respond to information spills by:

6.10.9.1.1. Assigning, in the incident response plan, personnel or roles with responsibility for responding to information spills;

6.10.9.1.2. Identifying the specific information involved in the information system contamination;

6.10.9.1.3. Alerting personnel identified in the incident response plan of the information spill using a method of communication not associated with the spill;

6.10.9.1.4. Isolating the contaminated information system or information system component;

6.10.9.1.5. Eradicating the information from the contaminated information system or component;

6.10.9.1.6. Identifying other information systems or information system components that may have been subsequently contaminated; and

6.10.9.1.7. Performing any additional actions defined in the incident response plan.

6.11. Maintenance

6.11.1. Procedures (Authority - DIR CC: MA-1)

1.1 LSCPA must:

6.11.1.1. Develop procedures to facilitate the implementation of the Maintenance policy and associated controls;

6.11.1.1.1. Review and update Maintenance procedures at a college-defined frequency; and

6.11.1.1.2. Designate an individual as responsible for managing, developing, documenting, and disseminating college Maintenance procedures related to the controls in this policy.

6.11.2. Controlled Maintenance (Authority - DIR CC: MA-2)

6.11.2.1. LSCPA must require information custodians to:

6.11.2.1.1. Schedule, document, and review records of maintenance, repair, and/or replacement on information system components in accordance with manufacturer or vendor specifications and/or college-defined requirements;

6.11.2.1.2. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the information system or information system components are serviced on site or removed to another location;

6.11.2.1.3. Explicitly approve the removal of the information system or information system components from college facilities for off-site maintenance, repair, and/or replacement;

6.11.2.1.4. Sanitize equipment to remove all information from associated media prior to removal from college facilities for off-site maintenance, repair, and/or replacement;

6.11.2.1.5. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair, and/or replacement actions; and

6.11.2.1.6. Update appropriate college maintenance records following maintenance, repair, and/or replacement actions.

6.11.3. Nonlocal Maintenance (Authority - DIR CC: MA-4)

6.11.3.1. LSCPA, directly or contractually, must:

6.11.3.1.1. Approve and monitor nonlocal maintenance and diagnostic activities;

6.11.3.1.2. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with college policy and documented in the security plan for the information system;

6.11.3.1.3. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

6.11.3.1.4. Maintain records for nonlocal maintenance and diagnostic activities; and

6.11.3.1.5. Terminate session and network connections when nonlocal maintenance is completed.

6.11.4. Maintenance Personnel (Authority - DIR CC: MA-5)

6.11.4.1. LSCPA must:

6.11.4.1.1. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

6.11.4.1.2. Verify that non-escorted personnel performing maintenance on information systems possess the required access authorizations; and

6.11.4.1.3. Designate college personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

6.12. Media Protection

6.12.1. Procedures (Authority - DIR CC: MP-1)

6.12.1.1. LSCPA must:

6.12.1.1.1. Develop procedures to facilitate the implementation of the Media Protection policy and associated controls;

6.12.1.1.2. Review and update Media Protection procedures at a college-defined frequency; and

6.12.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Media Protection procedures related to the controls in this policy.

6.12.2. Media Access (Authority - DIR CC: MP-2)

6.12.2.1. LSCPA must restrict access to college-defined types of digital and non-digital media to college-defined personnel or roles.

6.12.3. Media Sanitization & Review, Approve, Track, Document, and Verify (Authority - Texas Government Code (TGC) 441.185; DIR CC: MP-6, MP-6(1))

6.12.3.1. LSCPA must:

6.12.3.1.1. Sanitize college-defined system media prior to disposal, release out of institutional control, or release for reuse using college-defined sanitization techniques and procedures; and

6.12.3.1.2. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

6.12.3.2. LSCPA must review, approve, track, document, and verify media sanitization and disposal actions.

6.12.3.3. LSCPA must keep a record documenting the removal and completion of sanitization of media that stored confidential information with the following information:

- Date;
- Description of the item(s) and serial number(s);
- Inventory number(s);
- The process and sanitization tools used to remove the data or method of destruction; and
- The name and address of the organization to which the media were transferred.

6.12.4. Media Use (Authority - DIR CC: MP-7)

6.12.4.1. LSCPA must document and enforce a Standard defining at minimum:

6.12.4.1.1. The types of system media within scope of the Standard;

6.12.4.1.2. Whether and under what conditions, including on what information systems or information system components, the use of each type of system media is authorized, restricted, or prohibited; and

6.12.4.1.3. Controls required to use authorized types of system media.

6.12.4.2. Each component college must prohibit the use of portable storage devices in college systems when such devices have no identifiable owner.

6.13. Physical and Environmental Protection

6.13.1. Procedures (Authority - DIR CC: PE-1)

6.13.1.1. LSCPA must:

6.13.1.1.1. Develop procedures to facilitate the implementation of the Physical and Environmental Protection policy and associated controls;

6.13.1.1.2. Review and update Physical and Environmental Protection procedures at a college-defined frequency; and

6.13.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Physical and Environmental Protection procedures related to the controls in this policy.

6.13.2. Physical Access Authorizations (Authority - DIR CC: PE-2)

6.13.2.1. LSCPA must:

6.13.2.1.1. Develop, approve, and maintain a list of individuals with authorized access to facilities in which one or more college information systems reside;

6.13.2.1.2. Issue authorization credentials for facility access;

6.13.2.1.3. Review the access list detailing authorized facility access by individuals at a college-defined frequency; and

6.13.2.1.4. Remove individuals from the facility access list when access is no longer required.

6.13.3. Physical Access Control (Authority - DIR CC: PE-3)

6.13.3.1. LSCPA must:

6.13.3.1.1. Enforce physical access authorizations at college-defined entry and exit points to facilities in which one or more college information systems reside by:

- Verifying individual access authorizations before granting access to each facility; and
- Controlling ingress and egress to each facility using college-defined physical access control systems, which may include systems, devices, and/or guards;

6.13.3.1.2. Maintain physical access audit logs for college-defined entry and exit points;

6.13.3.1.3. Control access to areas within each facility designated as publicly accessible using college-defined controls;

6.13.3.1.4. Escort visitors and monitor visitor activity based on college-defined requirements;

6.13.3.1.5. Secure keys, combinations, and other physical access devices;

6.13.3.1.6. Inventory college-defined physical access devices at a college-defined frequency; and

6.13.3.1.7. Change combinations and keys:

- At a college-defined frequency; and/or
- When keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

6.13.4. Monitoring Physical Access (Authority - DIR CC: PE-6)

6.13.4.1. LSCPA must:

6.13.4.1.1. Monitor physical access to facilities in which one or more college information systems reside to detect and respond to physical security incidents;

6.13.4.1.2. Review physical access logs at a college-defined frequency and upon occurrence of college-defined events or potential indications of events; and

6.13.4.1.3. Coordinate results of reviews and investigations with the college incident response capability.

6.13.5. Visitor Access Records (Authority - DIR CC: PE-8)

6.13.5.1. LSCPA must:

6.13.5.1.1. Maintain visitor access records to facilities in which one or more college information systems reside for a college-defined period;

6.13.5.1.2. Review visitor access records at a college-defined frequency; and

6.13.5.1.3. Report anomalies in visitor access records to college-defined personnel.

6.13.6. Emergency Lighting (Authority - DIR CC: PE-12)

6.13.6.1. LSCPA must employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within facilities in which one or more college information systems reside.

6.13.7. Fire Protection (Authority - DIR CC: PE-13)

6.13.7.1. LSCPA must employ and maintain fire suppression and detection devices or systems for facilities in which one or more college information systems reside that are supported by an independent energy source.

6.13.8. Environmental Controls (Authority - DIR CC: PE-14)

6.13.8.1. LSCPA must:

6.13.8.1.1. Maintain temperature and humidity levels within facilities in which one or more college information systems reside at college-defined acceptable levels; and

6.13.8.1.2. Monitor environmental control levels at a college-defined frequency.

6.13.9. Water Damage Protection (Authority - DIR CC: PE-15)

6.13.9.1. LSCPA must protect facilities in which one or more college information systems reside from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

6.13.10. Delivery and Removal (Authority - DIR CC: PE-16)

6.13.10.1. LSCPA must:

6.13.10.1.1. Authorize and control college-defined types of information system components entering and exiting facilities in which one or more college information systems reside; and

6.13.10.1.2. Maintain records of college-defined information system components.

6.13.11. Alternate Work Site (Authority - DIR CC: PE-17)

6.13.11.1. LSCPA must:

6.13.11.1.1. Determine and document college-defined alternate work sites allowed for use by employees;

6.13.11.1.2. Employ college-defined controls at alternate work sites;

6.13.11.1.3. Assess the effectiveness of controls at alternate work sites; and

6.13.11.1.4. Provide a means for employees to communicate with information security personnel in case of incidents.

6.14. Security Planning

6.14.1. Procedures (Authority - DIR CC: PL-1, TAC 202.73)

6.14.1.1. LSCPA must:

6.14.1.1.1. Develop procedures to facilitate the implementation of the Security Planning policy and associated controls;

6.14.1.1.2. Review and update Security Planning procedures at a college-defined frequency; and

6.14.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Security Planning procedures related to the controls in this policy.

6.14.1.2. Each component college’s information security officer must report annually on the college’s information security program to their respective college head in compliance with 1 Texas Administrative Code §202.73(a).

6.14.2. System Security and Privacy Plans (Authority - DIR CC: PL-2)

6.14.2.1. LSCPA must ensure that each information system under the college’s custodianship has a corresponding System Security Plan that:

6.14.2.1.1. Is consistent with the college's enterprise architecture;

6.14.2.1.2. Explicitly defines the constituent information system component(s);

6.14.2.1.3. Describes the function and security posture of the information system, including in terms of mission and business processes;

6.14.2.1.4. Provides the security categorization of the information system and highest classification of information it stores, processes, and/or transmits, including supporting rationale;

6.14.2.1.5. Describes any specific threats to the information system that are of concern to the college;

6.14.2.1.6. Describes the operational environment for the information system and relationships with or connections to other information systems;

6.14.2.1.7. Provides an overview of the security requirements for the information system that identifies the security controls in place;

6.14.2.1.8. Identifies any relevant security control baselines and, if applicable, college-defined overlays;

6.14.2.1.9. Describes the controls in place or planned for meeting the security requirements, including a rationale for any tailoring decisions;

6.14.2.1.10. Includes risk determinations for security architecture and design decisions;

6.14.2.1.11. Includes in a plan of action and milestones security-related activities affecting the information system that require planning and coordination with college-defined individuals or groups; and

6.14.2.1.12. Is reviewed and approved by the information owner prior to plan implementation.

6.14.2.2. Copies of the System Security Plan and subsequent changes to the plan must be distributed to relevant stakeholders.

6.14.2.3. LSCPA must review and update System Security Plans on a recurring basis. This review must occur at a college-defined frequency or when changes to the information system or System Security Plan require it.

6.14.2.4. System Security Plans must be protected from unauthorized disclosure and modification.

6.14.3. Rules of Behavior & Social Media and External Site/Application Usage Restrictions (Authority - DIR CC: PL-4, PL-4(1))

6.14.3.1. LSCPA must:

6.14.3.1.1. Establish and provide to users (including, but not limited to, state agency personnel, temporary employees, and employees of independent contractors) an acceptable use policy for college information resources that describes the users' responsibilities and expected behavior for the usage and security of information and Information Resources;

6.14.3.1.2. Periodically review and update the college acceptable use policy;

6.14.3.1.3. Require college users to acknowledge the acceptable use policy and indicate that the users have read, understand, and agree to abide by the acceptable use policy before authorizing access to the information and Information Resources; and

6.14.3.1.4. Require individuals who have acknowledged a previous version of the acceptable use policy to read and re-acknowledge when rules are revised or updated or at least annually as part of mandatory cybersecurity training.

6.14.3.2. LSCPA must include in the rules of behavior restrictions on:

6.14.3.2.1. Use of social media, social networking sites, and external sites/applications;

6.14.3.2.2. Posting college information on public websites; and

6.14.3.2.3. Use of college-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

6.14.4. Baseline Selection (Authority - DIR CC: PL-10)

6.14.4.1. LSCPA must:

6.14.4.1.1. Select a control baseline for information systems; and

6.14.4.1.2. Use the controls contained in the DIR Security Controls Standards Catalog as the default baseline for information systems.

6.14.5. Baseline Tailoring (Authority - DIR CC: PL-11)

6.14.5.1. LSCPA must tailor the selected control baseline by applying college-defined tailoring actions.

6.14.6. Data Classification, Security, and Retention Requirements for Information Resources Technology Projects (Authority – §TGC 2054.161)

6.14.6.1. On initiation of an information resources technology project, including an application development project and any information resources projects described in subchapter G of Texas Government Code §2054, the college shall classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements under Texas Government Code §441.185 for each classification.

6.14.7. Content of Rules of Behavior (Authority – TSUS Board of Regents)

6.14.7.1. LSCPA's rules of behavior must address, at minimum, the rules established in this section.

6.14.7.2. College vs. Individual Purpose

6.14.7.2.1. Users accessing college information resources are responsible for ensuring that their use of these resources is primarily for college purposes and college-related activities.

6.14.7.2.2. Access to information resources carries with it the responsibility for maintaining the security of the college's information resources.

6.14.7.2.3. Rules for incidental use of college information resources.

6.14.7.2.4. Individuals with authorized access to information resources must ensure that their access permissions are not accessible to or usable by any other individuals.

6.14.7.3. Personal vs. Official Representation

6.14.7.3.1. Students, faculty, and staff using information resources to reflect the ideas, comments, and opinions of individual members of the college community must be distinguished from those that represent the official positions, programs, and activities of the college.

6.14.7.3.2. Students, faculty, and staff using information resources for purposes of exchanging, publishing, or circulating official college documents must follow college requirements concerning appropriate content and style.

6.14.7.3.3. The college is not responsible for the personal ideas, comments, and opinions of individual members of the college community expressed through the use of college information resources.

6.14.7.4. Limitations on the Availability of Information Resources

6.14.7.4.1. The college's information resources are finite by nature. All members of the college community must recognize that certain uses of college information resources may be limited or regulated as required to fulfill the college's primary teaching and public service missions. Examples of these limitations include those related to capacity management, performance optimization, or security of the college's other information resources.

6.14.7.5. Privacy and Confidentiality of Electronic Documents

6.14.7.5.1. No information system can absolutely guarantee the privacy or confidentiality of electronic documents.

6.14.7.5.2. Information resources provided by the TSUS and LSCPA are essentially owned, respective of established copyright and intellectual law and TSUS and college policy, by the State of Texas and subject to state oversight. Consequently, persons have no right to privacy in their use of college information resources even when using a personal or third-party device to access such resources.

6.14.7.5.3. LSCPA should take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons using college information resources that the college will not seek access to their electronic messages or documents without their prior consent except where necessary to:

- Satisfy the requirements of the Texas Public Information Act, or other statutes, laws, or regulations;
- Allow college officials to fulfill their responsibilities when acting in their assigned capacity;
- Protect the integrity of the college's information resources, and the rights and other property of the college;

- Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations; or
- Protect the rights of individuals working in collaborative situations where information and files are shared.

6.14.7.5.4. LSCPA should establish procedures for appropriately preserving the privacy of information resources and for determining the methodology by which non-consensual access to information resources will be pursued by the college.

6.14.7.6. Failure to Comply with Information Technology Policies

6.14.7.6.1. Failure to adhere to the provisions of TSUS IT policies or the IT policies of LSCPA may result in:

- Suspension or loss of access to college information resources;
- Removal of elevated privileges to college information resources;
- Appropriate disciplinary action under existing procedures applicable to college users; and
- Civil or criminal prosecution.

6.14.7.7. To preserve and protect the integrity of information resources, there may be circumstances where the college must immediately suspend or deny access to the resources. Should an individual’s access be suspended under these circumstances, the college shall strive to inform the individual in a timely manner and afford the individual an opportunity to respond. The college shall then determine what disciplinary action is warranted and shall follow the procedures established for such cases.

6.15. Program Management

6.15.1. Information Security Program Plan (Authority - DIR CC: PM-1)

6.15.1.1. LSCPA must:

6.15.1.1.1. Develop and disseminate a college-wide information security program plan that:

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Includes the identification and assignment of roles, responsibilities, management commitment, coordination among college entities, and compliance;
- Reflects the coordination among college entities responsible for information security; and
- Is approved by a senior official with responsibility and accountability for the risk being incurred to college

operations (including missions, functions, image, and reputation), college assets, and individuals;

6.15.1.1.2. Review the college-wide information security program plan at a college-defined frequency;

6.15.1.1.3. Update the information security program plan to address institutional changes and problems identified during plan implementation or control assessments; and

6.15.1.1.4. Protect the information security program plan from unauthorized disclosure and modification.

6.15.2. Information Security Program Leadership Role (Authority - DIR CC: PM-2, Texas Administrative Code (TAC) 202.71, TAC 202.74)

6.15.2.1. LSCPA must:

6.15.2.1.1. Appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a college-wide information security program approved by the college's President or delegate.

6.15.2.1.2. LSCPA's senior information security officer is charged with the responsibilities enumerated at Texas Government Code §2054.136 and 1 Texas Administrative Code §202.71.

6.15.3. Information Security Resources (Authority - DIR CC: PM-3)

6.15.3.1. LSCPA must:

6.15.3.1.1. Include the resources needed to implement the information security program in capital planning and investment requests and document all exceptions to this requirement;

6.15.3.1.2. Prepare documentation required for addressing the information security program in capital planning and investment requests in accordance with applicable laws, regulations, policies and standards; and

6.15.3.1.3. Make available for expenditure, the planned information security resources.

6.15.4. Plan of Action and Milestones Process (Authority - DIR CC: PM-4)

6.15.4.1. LSCPA must:

6.15.4.1.1. Implement a process to ensure that plans of action and milestones for the information security program and associated college information systems:

- Are developed and maintained;
- Document the remedial information security actions to adequately respond to risk to college operations and assets, individuals, and other organizations; and
- Are reported in accordance with college-defined reporting requirements.

- Review plans of action and milestones for consistency with the college risk management strategy and college-wide priorities for risk response actions.

6.15.5. Information System Inventory (Authority - DIR CC: PM-5)

6.15.5.1. LSCPA must develop and update, on a college-defined frequency, an inventory of college information systems.

6.15.6. Information Security Measures of Performance (Authority - DIR CC: PM-6)

6.15.6.1. LSCPA must develop, monitor, and report to college-defined individuals on the results of information security measures of performance.

6.15.7. Enterprise Architecture (Authority - DIR CC: PM-7)

6.15.7.1. LSCPA must develop an enterprise architecture with consideration for information security and the resulting risk to college operations, college assets, individuals, and other organizations.

6.15.8. Risk Management Strategy (Authority - DIR CC: PM-9)

6.15.8.1. LSCPA must:

6.15.8.1.1. Develop a comprehensive strategy to manage:

- Security risk to college operations and assets, individuals, and other college information systems; and
- Privacy risk to individuals resulting from the authorized processing of personally identifiable information.

6.15.8.1.2. Implement the risk management strategy consistently across the college; and

6.15.8.1.3. Review and update the risk management strategy on a college-defined frequency or as required to address college changes.

6.15.9. Authorization Process (Authority - DIR CC: PM-10)

6.15.9.1. LSCPA must:

6.15.9.1.1. Manage the security of college information systems and the environments in which those systems operate through authorization processes;

6.15.9.1.2. Designate individuals to fulfill specific roles and responsibilities within the college risk management process; and

6.15.9.1.3. Integrate the authorization process into a college-wide risk management program.

6.15.10. Testing, Training, and Monitoring (Authority - DIR CC: PM-14)

6.15.10.1. LSCPA must:

6.15.10.1.1. Implement a process for ensuring that college plans for conducting security testing, training, and monitoring activities associated with college information systems:

- Are developed and maintained; and
- Continue to be executed; and

6.15.10.1.2. Review testing, training, and monitoring plans for consistency with the college risk management strategy and college-wide priorities for risk response actions.

6.15.11. Security Groups and Associations (Authority - DIR CC: PM-15)

6.15.11.1. LSCPA must establish and institutionalize contact with selected groups and associations within the information security community:

6.15.11.1.1. To facilitate ongoing information security education and training for college information security personnel;

6.15.11.1.2. To maintain currency with recommended information security practices, techniques, and technologies; and

6.15.11.1.3. To share current information security information, including threats, vulnerabilities, and incidents.

6.15.12. Threat Awareness Program (Authority - DIR CC: PM-16)

6.15.12.1. LSCPA must implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

6.15.13. Information Systems Governance and Management (Authority – TSUS ISO Council; TAC 202)

6.15.13.1. LSCPA must define a management framework which clearly delineates the roles and responsibilities for the management of college information systems.

6.15.13.2. At minimum, each LSCPA information system management framework must:

6.15.13.2.1. Delineate distinct roles for the information owner and information custodian of each information system;

6.15.13.2.2. Establish the responsibilities of information owners to include:

- Duties ascribed by TAC 202.72; and
- Assurance of compliance with state and college standards.

6.15.13.2.3. Establish the responsibilities of information custodians to include:

- Duties ascribed by TAC 202.72; and
- Assurance of compliance with state and college standards.

6.15.13.2.4. Establish the responsibilities of all information system users to, at minimum, require users to:

- Use the information system or other information resource only for the purpose specified by the college or information owner;
- Comply with information security controls and college policies, including those designed to prevent unauthorized or accidental disclosure, modification, or destruction of information and information resources; and

- Formally acknowledge that they will comply with the security policies and procedures in a method determined by the college President or their designated representative.

6.15.13.2.5. Incorporate threat and incident response procedures as specified in the TSUS Incident Response Policy.

6.15.13.2.6. Incorporate oversight measures including, but not limited to, obligations outlined in the TSUS "System and Services Acquisition" and "Risk Assessment" policies.

6.15.14. Network Governance and Management (Authority - TSUS ISO Council; TAC 202)

6.15.14.1. LSCPA must define a management framework which clearly delineates the roles and responsibilities for the management of college information networks.

6.15.14.2. At minimum, LSCPA's network management framework must:

6.15.14.2.1. Delineate distinct roles for the ownership and custodianship of the college's network;

6.15.14.2.2. Assign administration of the college network by the Information Resources Manager (IRM) or their designee;

6.15.14.2.3. Ensure owners, custodians, and users of the college network and the devices and information systems connected to the college network understand their accountability for such use, including, but not limited to, the Rules of Behavior as specified in the "Planning" TSUS IT Policy.

6.15.14.2.4. Incorporate design and architectural planning and coordination measures to, at minimum, include the following:

- Appropriate logical and/or physical segmentation of elements of the college network to promote sufficient separation of traffic based on security principles and performance purposes as authorized by each component institution's ISO.
- Fault tolerance in critical components of the network and upstream service providers to mitigate risks to network availability;
- College-defined procedures for the management of network-based security devices;
- Procedures for the management of public IP addresses assigned to the component institution by the American Registry for Internet Numbers (ARIN) and/or other external entities, including, at minimum, maintenance of up-to-date points of contact;
- College-defined procedures to ensure network devices or addresses that pose an immediate threat to network operations, performance, or other network-connected devices are disconnected or quarantined to minimize risk until the threat is permanently removed;

- College-defined procedures to ensure incident response actions comply with established, policy-defined controls and best practices regarding the preservation and treatment of forensic data;
- Adherence to the requirements set forth in the “Configuration Management” TSUS IT Policy;
- Implementation of safeguards as required by the “System and Communication Protection” TSUS IT Policy; and
- Procedures to regularly conduct security and risk assessments in alignment with relevant policies and laws, including the “Risk Assessment” TSUS IT Policy.

6.16. Personnel Security Policy

6.16.1. Procedures (Authority - DIR CC: PS-1)

6.16.1.1. LSCPA must:

6.16.1.1.1. Develop procedures to facilitate the implementation of the Personnel Security policy and associated controls;

6.16.1.1.2. Review and update Personnel Security procedures at a college-defined frequency; and

6.16.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Contingency Planning procedures related to the controls in this policy.

6.16.2. Position Risk Designation (Authority - DIR CC: PS-2)

6.16.2.1. LSCPA must:

6.16.2.1.1. Assign a risk designation to all college positions;

6.16.2.1.2. Establish screening criteria for individuals filling those positions; and

6.16.2.1.3. Review and update position risk designations at a college-defined frequency.

6.16.3. Personnel Screening (Authority - DIR CC: PS-3)

6.16.3.1. LSCPA must:

6.16.3.1.1. Screen individuals prior to authorizing access to information systems; and

6.16.3.1.2. Rescreen individuals when college-defined conditions require rescreening and where rescreening is indicated, the frequency of rescreening.

6.16.4. Personnel Termination (Authority - DIR CC: PS-4)

6.16.4.1. LSCPA, upon termination of an individual’s employment or employment-like affiliation (e.g., volunteers, contractors, guest lecturers, temporary workers, interns), must:

6.16.4.1.1. Disable information system access and terminate/revoke any authenticators and credentials associated with the individual within a college-defined time period;

6.16.4.1.2. Conduct exit interviews that include a discussion of college-defined information security topics that include review of any signed non-disclosure agreements and secure disposition of university data from personal devices in a manner stipulated by the college;

6.16.4.1.3. Retrieve all security-related, college information system-related property;

6.16.4.1.4. Retain access to college information and information systems formerly controlled by the terminated individual; and

6.16.4.1.5. Notify college-defined personnel within a college-defined time period.

6.16.4.2. LSCPA must establish procedures to sufficiently accommodate reasonably expected scenarios in which the controls in section 6.1 above cannot be fully executed upon the termination of an individual's employment (e.g., the termination of an employee who is also an actively enrolled student). At minimum, procedures must ensure that access and privileges associated with the terminated individual's employment or employment-like affiliation are removed even if the individual must retain access to information resources for other purposes.

6.16.5. Personnel Transfer (Authority - DIR CC: PS-5)

6.16.5.1. LSCPA must:

6.16.5.1.1. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems and facilities when individuals are reassigned or transferred to other positions within the college;

6.16.5.1.2. Initiate transfer or reassignment actions within a college-defined time period following the formal transfer action;

6.16.5.1.3. Modify access authorizations as needed to correspond with any changes in operational need because of reassignment or transfer; and

6.16.5.1.4. Notify college-defined personnel or roles within a college-defined time period.

6.16.6. Access Agreements (Authority - DIR CC: PS-6)

6.16.6.1. LSCPA must:

6.16.6.1.1. Develop and document access agreements for college information systems;

6.16.6.1.2. Review and update the access agreements at a college-defined frequency; and

6.16.6.1.3. Verify that individuals requiring access to college information and information systems:

- Sign appropriate access agreements prior to being granted access; and
- Re-sign access agreements to maintain access to college information systems when access agreements have been updated or at a college-defined frequency.

6.16.7. External Personnel Security (Authority - DIR CC: PS-7)

6.16.7.1. LSCPA must:

6.16.7.1.1. Establish personnel security requirements including security roles and responsibilities for external providers;

6.16.7.1.2. Require external providers to comply with personnel security policies and procedures established by the college;

6.16.7.1.3. Document personnel security requirements;

6.16.7.1.4. Require external providers to notify college-defined personnel or roles of any personnel transfers or terminations of external personnel who possess college credentials and/or badges, or who have information system privileges within a college-defined time period; and

6.16.7.1.5. Monitor provider compliance with personnel security requirements.

6.16.8. Personnel Sanctions (Authority - DIR CC: PS-8)

6.16.8.1. LSCPA must:

6.16.8.1.1. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

6.16.8.1.2. Notify college-defined personnel or roles within college-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

6.16.9. Position Descriptions (Authority - DIR CC: PS-9)

6.16.9.1. LSCPA must incorporate security roles and responsibilities into college position descriptions.

6.17. Risk Assessment

6.17.1. Procedures (Authority - DIR CC: RA-1)

6.17.1.1. LSCPA must:

6.17.1.1.1. Develop procedures to facilitate the implementation of the Risk Assessment policy and associated controls;

6.17.1.1.2. Review and update Risk Assessment procedures at a college-defined frequency; and

6.17.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Risk Assessment procedures related to the controls in this policy.

6.17.2. Security Categorization (Authority - DIR CC: RA-2, TAC 202.75, TAC 202.1)

6.17.2.1. The college's ISO must establish requirements for security categorization of information systems.

6.17.2.2. LSCPA must:

6.17.2.2.1. Categorize information systems, at a minimum of "high," "moderate," or "low," and in accordance with applicable laws, regulations and policies;

6.17.2.2.2. Identify and define college-appropriate information classification categories including, at minimum, the definition of "Confidential Information" as specified by 1 Texas Administrative Code Chapter 202, Subchapter A;

6.17.2.2.3. Document the security categorization results, including supporting rationale, in the system security plan for each information system; and

6.17.2.2.4. Verify that security categorization decisions are reviewed and approved by the authorizing official or the authorizing official's designated representative.

6.17.3. Risk Assessment & Supply Chain Risk Assessment (Authority - DIR CC: RA-3, RA-3(1); TAC 202.75, TAC 202.77; TGC 2054.0593)

6.17.3.1. LSCPA must:

6.17.3.1.1. Conduct an assessment of risk, including:

- The likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of each information system and the information processed, stored, and/or transmitted, and any related information;
- The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; and
- The identification of threats to and vulnerabilities in each information system;

6.17.3.1.2. Integrate risk assessment results and risk management decisions from the college and mission or business process perspectives with information system-level risk assessments;

6.17.3.1.3. Review and document risk assessment results in a report on a recurring, college-defined frequency;

6.17.3.1.4. Disseminate risk assessment results to college-defined personnel or roles;

6.17.3.1.5. Update the risk assessment at a college-defined frequency or when there are significant changes to information systems, environments of operation, or other conditions that may impact the security state of information systems; and

6.17.3.1.6. Ensure risk assessments are performed by information owners and supported by information custodians:

- At least biennially for systems containing confidential data;
- Periodically, at a frequency determined by the college, for systems containing non-confidential data; and
- When significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system occur.

6.17.3.2. LSCPA must:

6.17.3.2.1. Assess supply chain risks associated with college-defined systems, system components, and system services; and

6.17.3.2.2. Update the supply chain risk assessment at a college-defined frequency when there are significant changes to the relevant supply chain, or when changes to the system, environment of operation, or other conditions may necessitate a change in the supply chain.

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

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

6.17.3.3.2. The component college's President for all systems identified with a high residual risk.

6.17.4. Vulnerability Monitoring and Scanning & Update Vulnerabilities to be Scanned (Authority - DIR CC: RA-5, RA-5(2))

6.17.4.1. LSCPA must:

6.17.4.1.1. Monitor and scan for vulnerabilities in each information system and its hosted applications on a recurring frequency, at least annually, in accordance with the college's established process and when new vulnerabilities potentially affecting systems or applications are identified and reported;

6.17.4.1.2. Employ vulnerability monitoring and scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using college-defined standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and
- Measuring vulnerability impact;

6.17.4.1.3. Analyze vulnerability scan reports from vulnerability monitoring activities and results from security assessments;

6.17.4.1.4. Remediate legitimate vulnerabilities in a college-defined response time in accordance with a college assessment of risk;

6.17.4.1.5. Share information obtained from the vulnerability scanning and monitoring processes and security assessments with appropriate information system custodians in accordance with the college's internal dissemination procedures; and

6.17.4.1.6. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

6.17.4.2. LSCPA must update the information system vulnerabilities to be scanned when at least one of the following conditions are met:

6.17.4.2.1. At a college-defined frequency;

6.17.4.2.2. Prior to a new scan; and/or

6.17.4.2.3. When new vulnerabilities are identified and reported.

6.17.5. Public Disclosure Program (Authority - DIR CC: RA-5(11))

6.17.5.1. LSCPA must establish a public reporting channel for receiving reports of vulnerabilities in college information systems and information system components.

6.17.6. Risk Response (Authority - DIR CC: RA-7)

6.17.6.1. LSCPA must respond to findings from security assessments, monitoring, and audits in accordance with college risk tolerance.

6.18. System and Services Acquisition

6.18.1. Procedures (Authority - DIR CC: SI-1)

6.18.1.1. LSCPA must:

6.18.1.1.1. Develop procedures to facilitate the implementation of the Systems and Services Acquisition policy and associated controls;

6.18.1.1.2. Review and update System and Information Integrity procedures at a college-defined frequency; and

6.18.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college System and Services Acquisition procedures related to the controls in this policy.

6.18.2. Allocation of Resources (Authority - DIR CC: SA-2)

6.18.2.1. LSCPA must:

6.18.2.1.1. Determine high-level information security requirements for each information system or information system service in mission and business process planning;

6.18.2.1.2. Determine, document, and allocate the resources required to protect each information system or information system service as part of its capital planning and investment control process; and

6.18.2.1.3. Establish a discrete line item for information security in college programming and budgeting documentation.

6.18.3. System Development Life Cycle (Authority - DIR CC: SA-3)

6.18.3.1. LSCPA must:

6.18.3.1.1. Acquire, develop, and manage information systems using a college-defined system development life cycle that incorporates information security considerations;

6.18.3.1.2. Define and document information security roles and responsibilities throughout the system development life cycle;

6.18.3.1.3. Identify individuals having information security roles and responsibilities; and

6.18.3.1.4. Integrate the college information security risk management process into system development life cycle activities.

6.18.3.2. LSCPA must:

6.18.3.2.1. Include information security, security testing, and audit controls in all phases of the system development lifecycle or acquisition process.

6.18.4. Acquisition Process (Authority - DIR CC: SA-4, TGC §2054.138)

6.18.4.1. LSCPA must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for each information system, information system component, or information system service in accordance with applicable federal/state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and college mission/business needs:

6.18.4.1.1. Security functional requirements;

6.18.4.1.2. Strength of mechanism requirements;

6.18.4.1.3. Security assurance requirements;

6.18.4.1.4. Controls needed to satisfy the security requirements;

6.18.4.1.5. Security-related documentation requirements;

6.18.4.1.6. Requirements for protecting security-related documentation;

6.18.4.1.7. Description of the information system development environment and environment in which the system is intended to operate;

6.18.4.1.8. Allocation of responsibility or identification of parties responsible for information security and supply chain risk management; and

6.18.4.1.9. Acceptance criteria.

6.18.4.2. Each component college entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the component college shall include, within or as an addendum to the contract, the “Information Security and Accessibility Standards” Exhibit from the TSUS Contract Management Handbook or, if superseded, the appropriate addendum replacing the exhibit.

6.18.5. System Documentation (Authority - DIR CC: SA-5)

6.18.5.1. LSCPA must:

6.18.5.1.1. Obtain administrator documentation for each information system, information system component, or information system service that describes:

- Secure configuration, installation, and operation of the system, component, or service;
- Effective use and maintenance of security functions/mechanisms; and
- Known vulnerabilities regarding configuration and use of administrative or privileged functions;

6.18.5.1.2. Obtain user documentation for each information system, information system component, or information system service that describes:

- User-accessible security functions and mechanisms and how to effectively use those security functions/mechanisms;
- Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
- User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

6.18.5.2. Document attempts to obtain information system, information system component, or information system service documentation when such documentation is either unavailable or nonexistent and take college-defined actions in response;

6.18.5.3. Protect documentation as required, in accordance with the college risk management strategy; and

6.18.5.4. Distribute documentation to college-defined personnel or roles.

6.18.6. Security Engineering Principles (Authority - DIR CC: SA-8)

6.18.6.1. LSCPA must:

6.18.6.1.1. Define and establish college security engineering principles; and

6.18.6.1.2. Apply the security engineering principles in the specification, design, development, implementation, and modification of the information system and information system components.

6.18.7. External System Services (Authority - DIR CC: SA-9)

6.18.7.1. LSCPA must:

6.18.7.1.1. Require that providers of external information system services comply with college information security requirements and employ college-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

6.18.7.1.2. Define and document college oversight and user roles and responsibilities with regard to external information system services; and

6.18.7.1.3. Employ college-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

6.18.8. Developer Configuration Management (Authority - DIR CC: SA-10)

6.18.8.1. LSCPA must require the developer of each information system, information system component, or information system service to:

6.18.8.1.1. Perform configuration management during at least one of the following life cycle stages: design, development, implementation, operation, or disposal;

6.18.8.1.2. Document, manage, and control the integrity of changes to college-defined configuration items under configuration management;

6.18.8.1.3. Implement only college-approved changes to the information system, information system component, or information system service;

6.18.8.1.4. Document approved changes to the information system, information component, or information system service and the potential security impacts of such changes; and

6.18.8.1.5. Track security flaws and flaw resolution within the information system, information system component, or information system service and report findings to college-defined personnel.

6.18.8.2. LSCPA must require:

6.18.8.2.1. The information owner approve all security-related information resources changes for their respective information system(s) through a change control process; and

6.18.8.2.2. The approval of such changes to occur prior to the implementation of the security-related information resources changes by the college or independent contractors.

6.18.9. Developer Testing and Evaluation (Authority - DIR CC: SA-11)

6.18.9.1. LSCPA must require the developer of the information system, information system component, or information system service, at all post-design stages of the system development life cycle, to:

6.18.9.1.1. Develop and implement a plan for ongoing security assessments;

6.18.9.1.2. Perform the appropriate level and frequency of testing and evaluation based on the classification of data and the security categorization of the information system;

6.18.9.1.3. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

6.18.9.1.4. Implement a verifiable flaw remediation process; and

6.18.9.1.5. Correct flaws identified during testing and evaluation.

6.18.10. Unsupported System Components (Authority - DIR CC: SA-22)

6.18.10.1. LSCPA must:

6.18.10.1.1. Replace information system components when support for the components is no longer available from the developer , vendor, or manufacturer; or

6.18.10.1.2. Provide alternative sources for continued support for unsupported components (e.g., support from external providers, in-house support if technically feasible).

6.19. System and Communications Protection

6.19.1. Procedures (Authority - DIR CC: SC-1)

6.19.1.1. LSCPA must:

6.19.1.1.1. Develop procedures to facilitate the implementation of the System and Communications Protection policy and associated controls;

6.19.1.1.2. Review and update System and Communications Protection procedures at a college-defined frequency; and

6.19.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college System and Communications Protection procedures related to the controls in this policy.

6.19.2. Denial of Service Protection (Authority - DIR CC: SC-5)

6.19.2.1. LSCPA must protect information systems against, or limit the effects of, college-defined types of denial-of-service attacks by employing college-defined safeguards.

6.19.3. Boundary Protection (Authority - DIR CC: SC-7)

6.19.3.1. LSCPA must:

6.19.3.1.1. Monitor and control communications at the external interfaces of each information system and at key internal interfaces within each information system;

6.19.3.1.2. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal college networks; and

6.19.3.1.3. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with a college security architecture.

6.19.3.2. The college President (or their designated representative) and the college's information security officer must establish a security strategy that includes perimeter protection. Perimeter security controls incorporated in the perimeter protection strategy may include and/or affect some or all of the following components:

6.19.3.2.1. Demilitarized Zone(s) (DMZ);

6.19.3.2.2. Firewall(s);

6.19.3.2.3. Intrusion detection system(s);

6.19.3.2.4. Intrusion prevention system(s); and

6.19.3.2.5. Router(s).

6.19.4. Transmission Confidentiality and Integrity (Authority - DIR CC: SC-8)

6.19.4.1. LSCPA must ensure that each information system protects the confidentiality and/or integrity of transmitted information.

6.19.4.2. LSCPA must:

6.19.4.2.1. Document in a Standard, based on college risk-management decisions, encryption requirements for data transmissions of confidential and non-confidential information and encryption key standards and management; and

6.19.4.2.2. Encrypt confidential information with, at minimum, a 128-bit encryption algorithm when the confidential information is transmitted over a public network (e.g., the Internet).

6.19.5. Cryptographic Key Establishment and Management (Authority - DIR CC: SC-12)

6.19.5.1. LSCPA must establish and manage cryptographic keys for required cryptography employed within each information system in accordance with college-defined requirements for key generation, distribution, storage, access, and destruction.

6.19.6. Cryptographic Protection (Authority - DIR CC: SC-13)

6.19.6.1. LSCPA must:

6.19.6.1.1. Determine college-defined cryptographic uses; and

6.19.6.1.2. Implement college-defined types of cryptography required for each specified cryptographic use.

6.19.7. Collaborative Computing Devices and Applications (Authority - DIR CC: SC-15)

6.19.7.1. LSCPA must:

6.19.7.1.1. Prohibit remote activation of collaborative computing devices and applications except for college-defined devices and applications; and

6.19.7.1.2. Provide an explicit indication of use to users physically present at the devices.

6.19.8. Secure Name / Address Resolution Service (Authoritative Source) (Authority - DIR CC: SC-20)

6.19.8.1. LSCPA must ensure that each information system that provides name resolution services:

6.19.8.1.1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the information system returns in response to external name/address resolution queries; and

6.19.8.1.2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

6.19.9. Secure Name / Address Resolution Service (Recursive or Caching Resolver) (Authority - DIR CC: SC-21)

6.19.9.1. LSCPA must ensure that each information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the information system receives from authoritative sources.

6.19.10. Architecture and Provisioning for Name / Address Resolution Service (Authority - DIR CC: SC-22)

6.19.10.1. LSCPA must ensure that information systems that collectively provide name/address resolution service for a component college are fault-tolerant and implement internal and external role separation.

6.19.11. Protection of Information at Rest (Authority - TSUS ISO Council: SC-28)

6.19.11.1. LSCPA must protect the confidentiality and/or integrity of college-defined types of information at rest.

6.19.11.2. LSCPA must:

6.19.11.2.1. Document in a Standard, based on college risk-management decisions, encryption requirements for information storage devices, as well as specific requirements for portable devices, removable media, and encryption key standards and management;

6.19.11.2.2. Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., a webserver or fileserver accessible without authentication or other access controls) must be encrypted;

6.19.11.2.3. Discourage the use of portable devices to store confidential information; and

6.19.11.2.4. Require that confidential information be encrypted if copied to or stored on:

- Endpoint computing devices not owned by a state agency;
- Portable computing devices (regardless of ownership); or
- Removable media (regardless of ownership).

6.19.12. Process Isolation (Authority - DIR CC: SC-39)

6.19.12.1. LSCPA must ensure that each information system maintains a separate execution domain for each executing process.

6.20. System and Information Integrity

6.20.1. Procedures (Authority - DIR CC: SI-1)

6.20.1.1. LSCPA must:

6.20.1.1.1. Develop procedures to facilitate the implementation of the System and Information Integrity policy and associated controls;

6.20.1.1.2. Review and update System and Information Integrity procedures at a college-defined frequency; and

6.20.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college System and Information Integrity procedures related to the controls in this policy

6.20.2. Flaw Remediation (Authority - DIR CC: SI-2)

6.20.2.1. LSCPA must:

6.20.2.1.1. Identify, report to college personnel or roles with information security responsibilities, and correct information system flaws;

6.20.2.1.2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

6.20.2.1.3. Install security-relevant software and firmware updates within a college-defined time period of the release of the updates; and

6.20.2.1.4. Incorporate flaw remediation into the college configuration management process.

6.20.3. Malicious Code Protection (Authority - DIR CC: SI-3)

6.20.3.1. LSCPA must:

6.20.3.1.1. Implement, signature-based and/or non-signature based malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

6.20.3.1.2. Automatically update malicious code protection mechanisms as new releases are available in accordance with college configuration management policy and procedures;

6.20.3.1.3. Configure malicious code protection mechanisms to:

- Perform periodic scans of information systems at a college-defined frequency and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with college security policy; and
- Perform one or more of the following in response to malicious code detection: block malicious code; quarantine malicious code; send an alert to college-defined personnel or roles; and/or perform another college-defined action.

6.20.3.1.4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of information systems.

6.20.4. Information System Monitoring (Authority - DIR CC: SI-4)

6.20.4.1. LSCPA must:

6.20.4.1.1. Monitor each information system to detect:

- Attacks and indicators of potential attacks in accordance with college-defined monitoring objectives; and
- Unauthorized local, network, and remote connections;

6.20.4.1.2. Identify unauthorized use of information systems through college-defined techniques and methods;

6.20.4.1.3. Deploy monitoring devices and/or invoke internal monitoring capabilities:

- Strategically within information systems to collect college-defined essential information; and
- At ad hoc locations within information systems to track specific types of transactions of interest to the college;

6.20.4.1.4. Analyze detected events and anomalies;

6.20.4.1.5. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

6.20.4.1.6. Adjust the level of information system monitoring activity whenever there is a change in risk to college operations and assets, individuals, or other organizations;

6.20.4.1.7. Obtain legal opinion regarding information system monitoring activities; and

6.20.4.1.8. Provide college-defined information system monitoring information to college-defined personnel or roles as needed and/or at a college-defined frequency.

6.20.5. Security Alerts, Advisories, and Directives (Authority - DIR CC: SI-5)

6.20.5.1. LSCPA must:

6.20.5.1.1. Receive information system security alerts, advisories, and directives from college-defined external organizations on an ongoing basis;

6.20.5.1.2. Generate internal security alerts, advisories, and directives as deemed necessary;

6.20.5.1.3. Disseminate security alerts, advisories, and directives to college-defined personnel or roles, college-defined elements within the college, and/or college-defined external organizations; and

6.20.5.1.4. To the extent required by law or other regulations, implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

6.20.6. Information Input Validation (Authority - DIR CC: SI-10)

6.20.6.1. LSCPA must ensure that each information system checks the validity of college-defined information inputs.

6.20.7. Information Management and Retention (Authority - DIR CC: SI-12)

6.20.7.1. LSCPA must manage and retain information within each information system and information output from each information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and operational requirements.

6.21. Supply Chain Risk Management

6.21.1. Procedures (Authority - DIR CC: SR-1)

6.21.1.1. LSCPA must:

6.21.1.1.1. Develop procedures to facilitate the implementation of the Supply Chain Risk Management policy and associated controls;

6.21.1.1.2. Review and update Supply Chain Risk Management procedures at a college-defined frequency; and

6.21.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Supply Chain Risk Management procedures related to the controls in this policy.

6.21.2. Supply Chain Risk Management Plan (Authority - DIR CC: SR-2)

6.21.2.1. LSCPA must:

6.21.2.1.1. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of college-defined information systems, system components or system services;

6.21.2.1.2. Implement the supply chain risk management plan consistently across the college; and

6.21.2.1.3. Review and update the supply chain risk management plan at a college-defined frequency or as required, to address threat, organizational or environmental changes.

6.21.3. Supply Chain Controls and Processes (Authority - DIR CC: SR-3)

6.21.3.1. LSCPA must:

6.21.3.1.1. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of college-defined information systems or information system components in coordination with college-defined personnel or roles;

6.21.3.1.2. Employ college-defined supply chain controls to protect against supply chain risks to information systems, information system components, or information system services and to limit the harm or consequences from supply chain-related events; and

6.21.3.1.3. Document the selected and implemented supply chain processes and controls in security plans, supply chain risk management plan(s), and/or college-defined documents.

6.21.4. Acquisition Strategies, Tools, and Methods (Authority - DIR CC: SR-5)

6.21.4.1. LSCPA must:

6.21.4.1.1. Employ college-defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

6.21.5. Notification Agreements (Authority - DIR CC: SR-8)

6.21.5.1. LSCPA must:

6.21.5.1.1. Establish agreements and procedures with entities involved in the supply chain for information systems, information system components, or information system services for the one or more of the following:

- Notification of supply chain compromises;
- Results of assessments or audits; and/or
- College-defined information and controls.

6.21.6. Component Disposal (Authority - DIR CC: SR-12)

6.21.6.1. LSCPA must:

6.21.6.1.1. Dispose of college-defined data, documentation, tools, and/or information system components using college-defined techniques and methods.

6.22. Exceptions

6.22.1. Pursuant to TAC 202.71 (c), the Lamar State College Port Arthur Information Security Officer, with the approval of the college President, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

6.23. Related Policies, Regulations, Standards, and Guidelines

6.23.1. Texas DIR Security Control Standards Catalog

6.23.2. 1 Tex. Admin. Code §202.76

6.23.3. LSCPA Information Resources Policy 1.0 Information Resources Management

6.23.4. LSCPA Information Resources Policy 2.0 Appropriate Use of Information Resources

6.23.5. LSCPA Information Resources Policy 4.0 College Websites

6.23.6. LSCPA Information Resources Policy 5.0 Information Security Program

POLICY: 7.0 LAPTOP LOAN PROGRAM
SCOPE: STAFF AND STUDENTS
APPROVED: August 2021
REVISED:

7.1. Policy Statement

7.1.1. Lamar State College Port Arthur provides laptops for the purpose of participating and successfully completing coursework.

7.1.2. The Laptop Loan Program policy establishes the Laptop Loan Program, which provides students with the opportunity to borrow a laptop for an extended period of time.

7.1.3. Students must meet the eligibility criteria in order to participate in the Laptop Loan Program.

7.1.4. The Laptop Loan Program includes laptops, power cables, and standard installed software (hereafter referred to as “equipment”).

7.1.5. Equipment availability is limited and will be made available to eligible students on a first come first serve basis.

7.1.6. Applications may be submitted 30 days prior to the first day of class. Equipment will be issued beginning on the first day of class.

7.2. Eligibility

7.2.1. In order to be considered, students must meet the following criteria:

7.2.1.1. Must be enrolled at LSCPA in credit-bearing or developmental courses or a dual-enrolled student from an ISD that does not issue computing devices.

7.2.1.2. Tuition, fees, and other charges for the current and previous semesters must be paid in full, or satisfactory payment arrangements must be made with the Business Office.

7.3. Use of Equipment

7.3.1. Equipment may be used by the student to whom the laptop is assigned. Equipment may not be loaned or shared with others, including family members or other LSCPA students.

7.3.2. Students must not alter or tamper with security settings or equipment hardware.

7.3.3. Students must not install unauthorized software.

7.3.4. Equipment must not be used for any form of illegal or illicit activities (e.g., hacking, pirating, viewing or downloading illegal or illicit content, etc.). If the equipment is used for any illegal activities while under the student’s control, the student may be subject to disciplinary action by the College, determined to be ineligible to participate in the Laptop Loan Program, as well as referral to legal and law enforcement agencies.

7.3.5. Other violations of policy or abuse of equipment privileges may also result in disciplinary action and the inability to borrow equipment in the future.

7.4. Returning Equipment

7.4.1. Students must return the equipment before the last day of the semester when the equipment was loaned to the student.

7.4.2. If a student withdraws completely from LSCPA or stops attending all of their courses, the equipment must be returned immediately. Failure to return the equipment will be considered failure to return LSCPA property and appropriate action will be taken.

7.4.3. It is expected that equipment will be returned in good working condition. If not, damage to the equipment will be assessed and charged to the LSCPA student account.

7.4.4. Failure to return equipment may result in one or more of the following:

7.4.4.1. The cost of replacing equipment will be assessed a dollar amount no greater than actual cash value as determined by LSCPA.

7.4.4.2. The cost of unreturned equipment will be charged to the LSCPA student account.

7.4.4.3. The student may be subject to disciplinary action by the College.

7.4.4.4. The student may be determined to be ineligible to participate in the Laptop Loan Program.

7.4.4.5. The student may be referred to legal and law enforcement agencies

7.4.5. Charges that are accrued through the Laptop Loan Program will result in a hold put on the LSCPA student account and will prevent the student from registering for a future term, receiving an official transcript, or receiving a diploma until paid in full. If the balance is not paid in full, it will be referred to collections.

7.5. Related Policies, Regulations, Standards, and Guidelines

7.5.1. Information Resources Policy 2.0 Appropriate Use of Information Resources

POLICY: **8.0 USE OF CLOUD SERVICES**
SCOPE: **FACULTY AND STAFF**
APPROVED: **August 2021**
REVISED:

8.1. Policy Statement

The Use of Cloud Services Policy establishes a framework for the use of Cloud Services to ensure that LSCPA data is appropriately stored, processed, shared, and managed on those services.

8.2. Application

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

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

8.2.3. Information that is used solely for classroom instruction purposes (e.g., lecture notes or PowerPoint slides for teaching) is not covered under this policy, provided it is not classified as Confidential, Sensitive, or Regulated (see Information Resources Policy 5.5 Data Classification).

8.3. General Information

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

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

8.3.3. Cloud Services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. The college must determine how data would be recovered.

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

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

8.4. Cloud Computing Service Providers Eligibility / Approval

8.4.1. Cloud Service Providers must be approved by the IRM and ISO.

8.4.2. Cloud Services usage involves delegating custody and aspects of data security to the Cloud Service Provider, Cloud Service Providers that will be used to store, process, share, or manage college data classified as Confidential, Sensitive, or Regulated, must be contractually obligated with LSCPA to assume the appropriate delegated responsibilities.

8.4.3. The IRM shall maintain a list of approved Cloud Service Providers. Providers shall be selected based on data classification.

8.4.4. LSCPA provides employees with cloud-based services such as Office 365, OneDrive, and Microsoft Teams, which can be accessed from both on campus and off campus computing devices.

8.4.4.1. Computing devices not under the direct control of the user or LSCPA (e.g., public-use computers in libraries, hotels, and other locations) may not be used to access Confidential, Sensitive, or Regulated data.

8.5. Personal Cloud Computing Services

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

8.6. Exceptions

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

APPENDICES

APPENDIX A: Acronyms

BCC	Business and Commerce Code
BCP	Business Continuity Plan
COOP	Continuity of Operations Plan
DIR	Department of Information Resources
DIR CC	Department of Information Resources Controls Catalog
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
EIR	Electronic and Information Resources
IRM	Information Resources Manager
ISO	Information Security Officer
ITS	Information Technology Services
MS-ISAC	Multi-State Information Sharing & Analysis Center
NIST	National Institute of Standards and Technology
PII	Personal Identifying Information, Personally Identifiable Information
PIN	Personal Identification Number
SSP	System Security Plan
TAC	Texas Administrative Code
TGC	Texas Government Code
TRAIL	Texas Records and Information Locator
VPAT	Voluntary Product Accessibility Template
WCAG	Web Content Accessibility Guidelines

APPENDIX B: Glossary

Access - The physical or logical capability to view, interact with, or otherwise make use of Information Resources.

Acceptable Risk - The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific information system.

Access Control - The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., data centers, physical plant, mechanical rooms, Network closets, secured buildings, and research laboratories).

Accessible - Describes an electronic and information resource that can be used in a variety of ways and (the use of which) does not depend on a single sense or ability.

Account - A mechanism relating to identity that provides access to an information system or network.

Acquisition - Includes all stages of the process of acquiring products or services, beginning with the process for determining the need for the product or service and ending with contract completion and closeout.

Administrative Access - Privileged access that bypasses user-level controls in order to manage the information system.

Administrative Privileges - Rights granted to a Privileged User.

Alternate Formats - Alternate formats usable by people with disabilities may include, but are not limited to, Braille, ASCII text, large print, recorded audio, and electronic formats that comply with this chapter.

Alternate Methods - Different means of providing information, including product documentation, to people with disabilities. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text to-speech synthesis, and audio description.

Assistive Technology - Any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.

Attribute - A claim of a named quality or characteristic inherent in or ascribed to someone or something.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational Procedures.

Audit Log / Audit Records - A chronological record of Information System activities, including records of system Accesses and operations performed in a given period.

Auditable Event - Events which are significant and relevant to the security of Information Systems and the environments in which those systems operate in order to meet specific and ongoing Audit needs. Audit events can include, for example, Password changes, failed logons, or failed accesses related to Information Systems, Administrative Privilege usage, or third-party credential usage.

Authentication - Verifying the Identity of a User, process, or Device, often as a prerequisite to allowing Access to resources in an Information System.

Authenticator - The means used to confirm the Identity of a User, process, or Device (e.g., User Password or token).

Authorization - The right or a permission that is granted to a system entity to access a system resource.

Authorization Boundary - All components of an Information System to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the Information System is connected.

Authorizing Official (AO) – See “Information Owner”.

Availability - The security objective of ensuring timely and reliable Access to and use of information.

Backup - A copy of files and programs made to facilitate recovery, if necessary.

Baseline Configuration - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures

Best Practice - See Guideline.

Boundary Protection Device - A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or Procedures that describe how the institution’s mission/business processes will be sustained during and after a significant disruption.

Business Function - Process or operation performed routinely to carry out a part of the mission of an institution.

Business Impact Analysis (BIA) - An analysis of an Information System’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Certificate Authority - The entity in a Public Key Infrastructure (PKI) that is responsible for issuing public-key certificates and exacting compliance to a PKI policy. Also known as a Certification Authority.

Cloud Computing - A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. For the purpose of this Policy, Cloud Computing encompasses any computing, software services, hosting environment, or storage environment that is not directly owned and controlled by LSCPA.

Cloud Service Provider - A vendor that offers Cloud Services.

Cloud Services - Services utilizing Cloud Computing technologies that are available via the Internet and are managed by third parties. Examples of cloud services include, but are not limited to, Internet-based web applications, commercial email and other messaging, document storage and cloud platforms and infrastructure.

Collaborative Computing Device - Tools that facilitate and enhance group work through distributed technology - where individuals collaborate from separate locations. Devices can include but are not limited to Networked white boards, cameras, and microphones.

College Home Page - The web page that displays when www.lamarpa.edu is the URL.

College Websites - Websites and web pages owned or controlled by Lamar State College Port Arthur that represent the college.

Common Control - A security control that is inherited by one or more information systems.

Compensating Security Controls - The security controls employed in lieu of the recommended controls that provide equivalent or comparable protection.

Confidential Information - Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

Confidentiality - The security objective of preserving authorized restrictions on information Access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control - Process for controlling modifications to hardware, Firmware, software, and documentation to protect the Information System against improper modifications before, during, and after system implementation.

Configuration Management - A collection of activities focused on establishing and maintaining the Integrity of information technology products and Information Systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Configuration Settings - The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.

Content - The information and services delivered through a Web page or website.

Content Owner - A person who owns the responsibility for a website or web page, including the accuracy, timeliness, and appropriateness of all material and services resident at that website or web page.

Contingency Plan - Management policy and Procedures used to guide an institution response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the institutional Risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or disaster recovery plan (DRP) for major disruptions.

Continuity of Operations Plan (COOP) - See Business Continuity Plan.

Control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. A control may be technical or administrative in nature.

Control Assessment - See Security Assessment.

Cryptographic - Relating to the discipline that embodies the principles, means, and methods for the transformation of Data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Cryptographic Module - Any combination of hardware, Firmware or software that implements Cryptographic functions such as Encryption, Decryption, Digital Signatures, Authentication techniques and random number generation.

Cryptographic Module Authentication - The set of hardware, software, Firmware, or some combination thereof that implements Cryptographic logic or processes, including Cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Custodian - See Information Custodian.

Data - Information in a specific representation, usually as a sequence of symbols that have meaning.

Decryption - The process of changing ciphertext into plaintext using a Cryptographic algorithm and key.

Destruction - The result of actions taken to ensure that media cannot be reused as originally intended and that information is technologically infeasible to recover or prohibitively expensive.

Developer - A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

Device Administrator - An individual with principal responsibility for the installation, configuration, registration, security, and ongoing maintenance of a Network-connected Device.

Device Owner - The department head charged with overall responsibility for the Networking component in the institution’s inventory records. The Device Owner must designate an individual to serve as the primary Device Administrator and may designate a backup Device Administrator. All Network Infrastructure Devices, (e.g., Network cabling, routers, switches, wireless access points, and in general, any non-endpoint Device) shall be centrally owned and administered.

Digital Media - A form of electronic media where data are stored in digital (as opposed to analog) form.

Digital Signature - The result of a Cryptographic transformation of Data which, when properly implemented, provides the services of: 1. origin Authentication, 2. Data Integrity, and 3. signer non-repudiation.

DIR CC – The security control catalog (CC) authored by the Texas Department of Information Resources (DIR) which provides 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).

Disaster Recovery Plan (DRP) - A written plan for recovering one or more information systems in response to a major hardware or software failure or destruction of facilities.

Domain - An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Electronic and Information Resources (EIR) - Includes information technology and any equipment or interconnected system or subsystem of equipment used to create, convert, duplicate, or deliver data or information. EIR includes telecommunications products (such as telephones), information kiosks and transaction machines, web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, thermostats or temperature control devices, and medical equipment that contain information technology that is integral to its operation, are not information technology. If the embedded information technology has an externally available web or computer interface, that interface is considered EIR. Other terms such as, but not limited to, Information and Communications Technology (ICT), Electronic Information Technology (EIT), etc. can be considered interchangeable terms with EIR for purposes of applicability or compliance.

Electronic and Information Resources (EIR) Owner - The individual responsible for a business function who determines controls for and oversees the development, acquisition, and/or use of EIR supporting that business function.

Encryption - The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the Encrypted text that conceals the Data's original meaning.

Enterprise Architecture - A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.

Event - Any observable occurrence in an information system.

Execution Domain - Each Information System process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

External Information System Service - An Information System service that is implemented outside of the Authorization Boundary of the institutional Information System (i.e.; a service that is used by, but not a part of, the institutional Information System) and for which the institution typically has no direct control over the application of required security controls or the assessment of security control effectiveness. Examples include but are not limited to externally hosted or cloud-based Information Systems.

External Information System Service - An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Network - A Network not controlled by the institution.

Federal Information Processing Standards (FIPS) - A Standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Firewall - An inter-Network connection Device that restricts Data communication traffic between two connected Networks. A Firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a Network. Typically, Firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Firmware - Computer programs and Data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and Data cannot be dynamically written or modified during execution of the programs.

Guideline - Guidelines provide guidance for achieving additional positive outcomes. Guidelines are not compulsory unless explicitly stated, but they should still be followed when practicable. Guidelines can also be used as prescriptive or informational documents.

Hardware - The physical components of an information system.

Home Page - The initial page that serves as the front door or entry point to a state website.

Identification - The process of discovering the true Identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identifier - Unique Data used to represent a person’s Identity and associated Attributes. A name or a card number are examples of Identifiers. Note: This also encompasses non-person entities.

Identity - The set of Attributes by which an entity is recognizable and that, within the scope of an Identity manager’s responsibility, is sufficient to distinguish that entity from any other entity.

Impact - The effect on organizational operations, organizational assets, individuals, or other organizations of a loss of confidentiality, integrity, or availability of information or an information system.

Incident - See Security Incident.

Incident Response - The mitigation of violations of security policies and Best Practices.

Information - Data as processed, stored, or transmitted by a computer.

Information Custodian - A department, agency, or Third-Party Provider responsible for implementing the Information Owner-defined controls and Access to an Information Resource.

Information Owner - A person(s) with statutory or operational authority for specified information or Information Resources and with responsibilities assigned in TSUS and component institution policy.

- Information owners are responsible for ensuring the implementation of security controls required by component institution policies and standards.
- In consultation with the component institution's ISO and IRM, information owners may also prescribe and implement additional controls or overlays specific to the information or Information Resource(s) for which they have statutory or operational authority.

Information Resource Employee - Agency employees performing administrative, security, governance, or compliance activities on information technology systems. These types of employees generally have an occupational Category of "Information Technology" per the Texas State Auditor's Office or similar duties.

Information Resources - the 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. Information Resources include but are not limited to:

- all physical and logical components, wired or wireless, of the Institutional Network;
- any Device that connects to or communicates electronically via the Institutional Network, including computers, printers, and communication Devices, both portable and fixed;
- any fixed or portable storage Device or media, regardless of ownership, that contains institution Data;
- all Data created, collected, recorded, processed, stored, retrieved, displayed, or transmitted using Devices connected to the Institutional Network;
- all computer software and services licensed by the institution;
- support staff and services employed or contracted by the institution to deploy, administer, or operate the above-described resources or to assist the community in effectively using these resources;
- Devices, software, or services that support the operations of the institution, regardless of physical location (e.g.; SAAS, PAAS, IAAS, cloud services); and
- telephones, audio and video conferencing systems, phone lines, and communications systems provided by the institution.

Information Resources Management - The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by institutions.

Information Resources Manager (IRM) - A designated employee authorized to manage the College's information resources and charged with assuming the responsibilities identified in Texas Government Code §2054 Subchapter D.

Information Security - The protection of information and Information Systems from Unauthorized Access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, Integrity, and Availability.

Information Security Officer (ISO) - The individual designated by the institution head who has the explicit authority and the duty to administer Information Security requirements institution wide.

Information Security Program - The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.

Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Information Spill(age) - Security event that results in the transfer of information onto an information system not authorized to store or process that information or information of the spilled information's Security Classification.

Information System - An interconnected set of Information Resources that share a common functionality. An Information System normally includes, but is not limited to, hardware, software, Network Infrastructure, information, applications, communications and people.

Information System Components - All components of an Information System to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the Information System is connected.

Information System Entry and Exit Points - These include but are not limited to Firewalls, electronic mail Servers, web Servers, proxy Servers, Remote Access Servers, workstations, notebook computers, and mobile Devices.

Information System Owner - See Information Owner.

Information System Service - A capability provided by an information system that facilitates information processing, storage, or transmission.

Information Technology - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. The term includes computers (including desktop and laptop computers), ancillary equipment, desktop software, client-server software, mainframe software, web application software and other types of software, firmware and similar procedures, services (including support services) and related resources.

Institutional Elements - Organizations, departments, facilities, or personnel responsible for a particular system's process.

Institutional Network - the Data transport and communications infrastructure at the institution. It includes the campus backbone, local area networks, and all equipment connected to those Networks (independent of ownership).

Integrity - The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Intellectual Property - Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract properties has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.

Interconnection Security Agreement - A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.

Internal Network - A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

Internet - The single, interconnected, worldwide system of commercial, governmental, educational, and other computer Networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

Intranet - A computer Network, especially one based on Internet technology, that the institution uses for its own internal (and usually private) purposes and that is closed to outsiders.

ISO - See “Information Security Officer”.

Least Privilege - The principle that a security architecture should be designed so that each entity is granted the minimum system resources and Authorizations that the entity needs to perform its function.

Malicious Code - Rogue computer programs designed to inflict a magnitude of harm by diminishing the Confidentiality, Integrity and Availability of Information Systems and information.

Malware - Software or Firmware intended to perform an unauthorized process that will have adverse impact on the Confidentiality, Integrity, or Availability of an Information System. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of Malware.

Management Controls - The security controls (i.e., safeguards or countermeasures) for an Information System that focus on Risk Management and the management of Information System security.

Managed Interfaces - An interface within an Information System that provides boundary protection capability using automated mechanisms or Devices.

Media - Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Metadata - Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

Metrics - Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related Data.

Mission Critical - Information Resources defined by the owner or by the institution to be crucial to the continued performance of the mission. Unavailability of such Information Resources would result in more than an inconvenience. An event causing the unavailability of Mission Critical Information Resources would result in consequences such as: significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations.

Mobile Device - A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); and is powered on for extended periods of time with a self-contained power source. Mobile Devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include laptops, smart phones, tablets, smart watches, and e-readers.

Multifactor Authentication - Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator.

Network - Information System(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control Devices.

Network Address - A unique number associated with a Device’s Network connection used for the routing of traffic across the Internet or another Network. Also known as Internet Protocol Address or IP Address.

Network Infrastructure - The hardware and software resources of an entire Network that enable Network connectivity, communication, operations and management of an enterprise Network. It provides the communication path and services between Users, processes, applications, services and External Networks/the Internet. These include but are not limited to cabling, routers, switches, hubs, Firewall appliances, wireless access points, virtual private network (VPN) Servers, network address translators (NAT), proxy Servers, and dial-up Servers.

NIST - National Institute of Standards and Technology.

Node - A Device or object connected to a Network.

Nonlocal Maintenance - Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.

Non-organizational User - A User who is not an institutional User (including public Users).

Organizational Users - An institutional User that the institution deems to have an affiliation including, for example, faculty, staff, student, contractor, guest researcher, or individual detailed from another organization.

Password - A type of Authenticator comprised of a string of characters (letters, numbers, and other symbols) used to authenticate an Identity or to verify Authorization.

Penetration Testing - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

Personally Identifiable Information (PII) - A category of personal Identity information as defined by §521.002(a)(1), Business and Commerce Code.

Plan of Action and Milestones - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Portable Storage Device - An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Potential Impact - The loss of confidentiality, integrity, or availability that could be expected to have: (i) a limited adverse effect (low); (ii) a serious adverse effect (moderate); or (iii) a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

Private Key - A Cryptographic key, used with a Cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Privileged Account - An Information System account with approved Authorizations of a Privileged User.

Privileged User - A User that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary Users are not authorized to perform.

Procedure - An operational-level document that details actions needed to implement a security control, configure a solution, or complete a task. Some Procedures may be compulsory, and other Procedures may just be one way of doing something. Procedures specify “how” things need to be done.

Protected Health Information (PHI) - Individually identifiable health information about an individual, including demographic information, which relates to the individual's past, present, or future physical or mental health condition, provision of health care, or payment for the provision of health care.

Public Information - A category of information as defined by Texas Government Code §552.002.

Public Key - A cryptographic key used with a cryptographic algorithm that is uniquely associated with an entity and that may be made public.

Public Key Certificate - A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it.

Reconstitution - Returning Information Systems to fully operational states.

Recovery Point Objective (RPO) - The point in time to which Data must be recovered after an outage.

Recovery Time Objective (RTO) - The overall length of time an Information System's components can be in the recovery phase before negatively impacting the institution's mission or mission/business processes.

Regulated Information - Information that is controlled by a state or federal regulation or other 3rd party agreement. This includes but is not to limited Sensitive Personal Information as defined under the Texas Business and Commerce Code 521.002(a)(1) and 521.002(a)(2), data subject to regulation by the Payment Card Industry Data Security Standards, and Federal tax information.

Remote Access - Access to an institutional Information System by a User (or an Information System) communicating through an External Network (e.g., the Internet).

Removable Media - Portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).

Residual Risk - Portion of Risk remaining after security measures have been applied.

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Assessment - The process of identifying Risks to institutional operations (including mission, functions, image, reputation), institutional assets, individuals, other institutions, resulting from the operation of a system. Part of Risk Management, incorporates threat and Vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with Risk analysis.

Risk Management - The total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes Risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Tolerance - The degree of Risk or uncertainty that is acceptable to an institution.

Role-Based Access Control (RBAC) - Access Control based on User roles (i.e., a collection of Authorizations a User receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an institution. A given role may apply to a single individual or to several individuals.

Sanitization - Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

Security Assessment - The testing and/or evaluation of the management, operational, and technical security controls in an Information System to determine 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.

Security Categorization - The characterization of information or an Information System as high, moderate, or low based on an assessment of the potential impact that a loss of Confidentiality, Integrity, or Availability of such information or Information System would have on institutional operations, institutional assets, or individuals.

Security Category - See “Security Categorization”.

Security Classification - The categorization of information based on its need for Confidentiality, as determined by federal, state, local laws, policies or regulations.

Security Control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Control Assessments - See Security Assessment.

Security Incident - An event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.

Security Plan - Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See System Security Plan or Information Security Program Plan.

Self-Contained, Closed Products - Products that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. These products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar products.

Sensitive Information - Information that may be subject to release under the Texas Public Information Act but should be controlled to protect third parties. This includes data that meets the definition of Personally Identifiable information under the Texas Business and Commerce Code §521.002(a)(1) and §521.002(a)(2), such as employee records and gross salary information. Other examples include but are not limited to emails, voicemails, instant messages, internal communications, and departmental procedures that might reveal otherwise protected information.

Sensitive Personal Information (SPI) - A category of personal Identity information as defined by §521.002(a)(2), Texas Business and Commerce Code.

Separation of Duty - A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or Access privilege to perpetrate damaging fraud.

Server - A physical or virtual Device that performs a specific service or function on behalf of other Network Devices or Users.

Server Administrator - A type of Information Custodian designated by the Server Owner as responsible for performing Server Management functions.

Server Management - Functions associated with the oversight of Server operations. These include controlling User Access, establishing/maintaining security measures, monitoring Server configuration and performance, and Risk Assessment and mitigation.

Server Owner - An institution employee charged with overall responsibility for the Server asset in the college's inventory records.

Site Policies Page - A web page containing website policies or a link to each policy.

Software - Computer programs and associated data that may be dynamically written or modified during execution.

Standard - A tactical-level, compulsory requirement to use the same technology, method, security control, baseline, or course of action to uniformly achieve the goals set by policies. Standards specify "what" needs to be done.

Suspected Data Breach - Is any incident in which sensitive, confidential or otherwise protected Data in human or machine-readable form is put at Risk because of exposure to unauthorized individuals.

System Administrator - Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

System Level Information - Information that includes but is not limited to, system-state information, operating system and application software, and licenses.

System Security Plan (SSP) - Formal document that provides an overview of the security requirements for an Information System and describes the security controls in place or planned for meeting those requirements.

Third Party Providers - Service providers, staffing, integrators, vendors, telecommunications, and infrastructure support that are external to the institution.

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

TRAIL - Texas Records and Information Locator, or its successor, providing a method to do a statewide search.

Transaction Risk Assessment - An evaluation of the security and privacy required for an interactive web session providing public access to government information and services.

Unauthorized Access - A person gains logical or physical Access without permission to institutional Information Resources.

Unauthorized Disclosure - An event involving the exposure of information to entities not authorized access to the information.

Uninterruptable Power Supply (UPS) - A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.

User - An individual, process, or automated application authorized to access an Information Resource in accordance with federal and state law, institution policy, and the Information Owner's Procedures and rules.

User Level Information - Any information other than System Level Information.

Voluntary Product Accessibility Template (VPAT) - A vendor-supplied form for a commercial Electronic and Information Resource used to document its compliance with technical accessibility standards and specifications.

Vulnerability - Weakness in an Information System, system security Procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment - Systematic examination of an Information System or product to determine the adequacy of security measures, identify security deficiencies, provide Data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Web Page - Presentation of state website content, including documents and files containing text, graphics, sounds, video, or other content, that is accessed through a web browser.

Web Presence - A representation of Lamar State College Port Arthur in text, graphics, audio, video, and any other forms of communication on the Web.

Website - A set of related web pages that are prepared and maintained as a collection in support of a single purpose.

APPENDIX C: Web Accessibility Statement

Lamar State College Port Arthur's website exists in a form that is accessible to a broad range of access devices.

This site has been engineered using the recommendations of the Web Content Accessibility Guidelines (WCAG) 2.0. Following these guidelines will make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these. Following these guidelines will also often make Web content more usable to users in general.

To improve the accessibility of our Web site, we test any major redesign with screen readers and other tools. The results of these reviews are incorporated into the Web site. LSCPA currently uses various tools for site validation, and it is our goal to achieve WCAG 2.0 Level AA conformance and compliance with the criteria established by the state (1 Tex. Admin. Code §206 & 1 Tex. Admin. Code §213).

More information on WCAG 2.0 standards can be found at the following sites:

- **Web Content Accessibility Guidelines (WCAG) 2.0**
- **How to Meet WCAG 2 (Quick Reference)**

If you use assistive technology and the format of any material on our websites interfere with your ability to access the information, please use the following point(s) of contact for assistance. To enable us to respond in a manner most helpful to you, please indicate the nature of your accessibility problem, the preferred format in which to receive the material, the web address of the requested material, and your contact information.

Laurie Marcantel
Disability Services Coordinator
Voice: 409-984-6241
TDD: 409-984-6242
FAX: 409-984-6056
E-mail: marcantella@lamarpa.edu

Lamar State College Port Arthur is open to suggestions on how the accessibility of this website can be improved. Please contact the EIR Accessibility Coordinator to offer suggestions or comments.

Susan Cook
EIR Accessibility Coordinator
Assistant Director, Infrastructure Services
Office: MMED 208I
Voice: 409-984-6146
Email: itaccessibility@lamarpa.edu

APPENDIX D: Linking Notice

Linking to an LSCPA Website

Advance permission to link to LSCPA websites is not required as long as that linking does not infringe on the rights of the content owner or LSCPA. LSCPA reserves the right to change the URL and content of its subpages at any time without notice.

Some information on LSCPA's websites may be protected by trademark and copyright laws and otherwise protected as intellectual property. Protected intellectual property must be used in accordance with state and federal laws and must reflect the proper ownership of the intellectual property.

LSCPA's trade and/or service names and marks are protected by law and may not be used without the written consent. Therefore, do not capture our pages within your frames or otherwise present our content as your own.

Do not link to individual graphics or tables within our pages, especially in an effort to place the downloading burden on our servers. Such an action may be considered an inappropriate use of state resources.

Any link to our sites should be a full forward link that tales the client browser to our site unencumbered. The back button should return the visitor to the original site if the visitor wishes to back out.

Links to External Sites

LSCPA provides links to sites that are appropriate to our mission and goals and as a convenience to our site visitors.

Linking to an external website does not constitute an endorsement of the content, viewpoint, accuracy, opinions, policies, products, services, or accessibility of the site. Any mention of vendors, products, or services is for informational purposes only. LSCPA reserves the right to remove links to external sites if they are inaccurate, inactive, or inappropriate.

LSCPA does not enter into reciprocal link agreements although we provide links to sites that are appropriate to our mission and goals. Our creation of a link to a site does not obligate that site's owner to provide a link back to LSCPA.

Upon leaving a LSCPA website and linking to an external site, the policies governing the LSCPA website no longer apply and users are subject to the external site's policies. If you discover an error or otherwise wish to comment on the content of a linked site, you should contact the owner of the site.

Contact Information

If you have any questions about this policy, the practices of this site, or dealings with this website, you can contact us by email or by mail at:

Information Technology Services
Lamar State College Port Arthur
P.O. Box 310
Port Arthur, TX 77641

APPENDIX E: Website Privacy Notice

Lamar State College Port Arthur (LSCPA) is committed to protecting your personal privacy. We treat your privacy as we do our own.

This Privacy Statement discloses our information gathering and dissemination practices for our website, www.lamarpa.edu. The statement outlines the information we may collect, how we protect it, and how we may use that information.

1. Collection of Information

While using our web pages, you do not have to identify yourself or divulge personal information. We may collect general information from you that does not identify you personally. This may include data such as your IP address, the name of the web page from which you entered our site, and which of our web pages you visited and for how long, as well as other general behavioral data. We aggregate this information to help us better focus on the needs and interests of our visitors and improve the overall functionality of our website.

As you use our website, we will not collect any personal information including your name, street address, email address, and telephone number, unless you provide the information to us voluntarily.

2. Cookies

When you view our website, we may store some information on your computer in the form of a cookie. A "cookie" is a small file containing information that is placed on a user’s computer by a web server.

Cookies allow us to tailor our website to better match your interests and preferences. Usage of a cookie is in no way linked to any of your personally identifiable information while on our site. You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience all features and content of our website.

Any information that LSCPA web servers may store in cookies is used for internal purposes only. Cookie data is not used in any way that would disclose personally identifiable information to outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

3. Third-Party Content

We may utilize third party services to better provide you with information, but likewise, will never collect personally identifiable information or transfer it to these companies.

4. Logs and Network Monitoring

LSCPA maintains log files of all access to its site and also monitors network traffic for the purposes of site management. This information is used to help diagnose problems with the server and to carry out other administrative tasks. Log analysis tools are also used to create summary statistics to determine which information is of most interest to users, to identify system problem areas, or to help determine technical requirements.

Information such as the following is collected in these files:

- IP address: the IP address of the computer requesting access to the site
- User-Agent: the type of browser, its version, and the operating system of the computer requesting access (e.g., IE 11 for Windows, Safari/Firefox for MacOS)
- Referer: the web page the user came from
- System date: the date and time on the server at the time of access
- Full request: the exact request the user made

- Status: the status code the server returned, e.g., fulfilled request, file not found
- Content length: the size, in bytes, of the file sent to the user
- Method: the request method used by the browser (e.g., post, get)
- Universal Resource Identifier (URI): the location of the particular resource requested. (More commonly known as a URL.)
- Query string of the URI: anything after a question mark in a URI. For example, if a keyword search has been requested, the search word will appear in the query string.
- Protocol: the technical protocol and version used, i.e., http 1.1, ftp, etc.

The above information is not used in any way that would reveal personally identifying information to outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

5. Email and Form Information

If a member of the general public sends LSCPA an email message or fills out a web-based form with a question or comment that contains personally identifying information, that information will only be used to respond to the request and analyze trends. The message may be redirected to another person or office that is better able to answer your question. Such information is not used in any way that would reveal personally identifying information to outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

6. Links

This site contains links to other sites. LSCPA is not responsible for the privacy practices or the content of such websites.

7. Use and Sharing of Information

When you do provide us with personal data, we may use that information to contact you or provide you with information about a LSCPA service, event, or news.

We will not sell, share, or otherwise distribute your personally identifiable information to third parties, except as required by law. LSCPA is a public institution, some information collected from our website, server log information, emails, and web-based forms, may be subject to the Texas Public Information Act (TGC 552).

8. Your Consent to This Privacy Statement

By using our website, you signify that you agree with the terms of our current Privacy Statement as posted in this area of the web site. If you do not agree with any term in this Statement, please do not provide any personal information on this site. If you do not provide personal information on this site, you may not be able to do certain things like access particular areas of the site, request certain types of information, or send us email.

9. Our Commitment to Security

We maintain physical, electronic, and procedural safeguards to protect against the loss, misuse or alteration of the information under our control. Safeguards include restricted access to computer systems, firewalls, encryption, and secure authentication methods.

Only employees who need the information to perform a specific job are granted access to personally identifiable information.

10. Changes to this Statement

We may occasionally decide to change our privacy statement, especially as new features are added to our website. If there are changes to this statement, we will post those changes here so you are always aware of what information we collect, and how we use it.

11. How to Contact Us

If you have any questions about this privacy statement, the practices of this site, or dealings with this website, you can contact us by email or by mail at:

Information Technology Services
Lamar State College Port Arthur
P.O. Box 310
Port Arthur, TX 77641