Information Resources Policy Manual

Lamar State College Port Arthur

Member Texas State University System™

November 2020

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 3
1.1. Policy Statement 4
1.2. Definitions 4
1.3. Roles and Responsibilities 4
1.4. Information Resources Manager (IRM) 4
1.5. Information Security Officer (ISO) 5
1.6. Information Technology Services Department 5
1.7. General 5
1.8. Information Resources Policy Management 5
1.9. Information Resources Standards, Guidelines, and Procedures Management 6
1.10. Related Policies, Regulations, Standards, and Guidelines 6
POLICY: 2.0 APPROPRIATE USE OF INFORMATION RESOURCES 7
2.1. Policy Statement 7
2.2. Applicability 7
2.3. General 7
2.4. Inappropriate Uses of Information Resources 8
2.5. Responsibilities of Users 10
2.6. Access to College Information Resources by Auditors 11
2.7. Consequences for Failure to Adhere to this Policy 11
2.8. Related Policies, Regulations, Standards, and Guidelines 12
POLICY: 3.0 ELECTRONIC AND INFORMATION RESOURCES ACCESSIBILITY 14
3.1. Policy Statement 14
3.2. Definitions 14
3.3. Applicability 14
3.4. Roles and Responsibilities 14
3.5. Procurement 15
3.6. Accessibility Testing and Validation 16
3.7. Website and Web Application Accessibility 16
3.8. Exceptions 16
3.9. Accessibility Standards 17
3.10. Related Policies, Regulations, Standards, and Guidelines 17
POLICY: 4.0 COLLEGE WEBSITES 19
4.1. Policy Statements 19
4.2. Definitions 19
4.3. Applicability 19
4.4. Roles and Responsibilities 19
4.5. Design and Technical Requirements 20
4.6. Linking Requirements 20
4.7. Privacy 21
4.8. Exceptions 21

4.9. Related Policies, Regulations, Standards, and Guidelines 21
POLICY: 5.0 INFORMATION SECURITY PROGRAM 22
5.1. Policy Statement 22
5.2. Definitions 22
5.3. Roles and Responsibilities 22
5.4. General 26
5.5. Data Classification 27
5.6. Information Security Risk Management 27
5.7. Information Security Exceptions 27
5.8. Information Security Reporting 28
5.9. Related Policies, Regulations, Standards, and Guidelines 28
POLICY: 6.0 INFORMATION SECURITY CONTROL STANDARDS 30
6.1. Policy Statement 30
6.2. Definitions 30
6.3. Access Control 30
6.4. Awareness and Training 33
6.5. Audit and Accountability 34
6.6. Configuration Management 36
6.7. Contingency Planning 38
6.8. Identification and Authentication 39
6.9. Incident Response 41
6.10. Maintenance 44
6.11. Media Protection 45
6.12. Physical and Environmental Protection 45
6.13. Risk Assessment 48
6.14. Security Assessment and Authorization 49
6.15. System and Communications Protection 51
6.16. System and Information Integrity 53
6.17. System and Services Acquisition 54
6.18. System Security Planning 57
6.19. Exceptions 58
6.20. Related Policies, Regulations, Standards, and Guidelines 58
APPENDICES 59
APPENDIX A: Acronyms Used in this Document 60
APPENDIX B: Glossary 61
APPENDIX C: Web Accessibility Statement 70
APPENDIX D: Linking Notice 71
APPENDIX E: Website Privacy Notice 72

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:

6.1. Policy Statement

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.

6.2. 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. Access Control Policy and Procedures (AC-1)

6.3.1.1. LSCPA must establish, implement, and maintain access control procedures to ensure secure user access to College information and information systems.

6.3.1.2. The procedures must be reviewed on an annual basis and updated if necessary.

6.3.2. Account Management (AC-2)

6.3.2.1. The information owner and the Information Resources Manager (IRM) must identify and document in the information system security plan the types of information system accounts (e.g., individual user, shared, developer, temporary, service, etc.) to be created to support the organizational and business functions of the information system.

6.3.2.2. Each information system that uses login credentials must have a designated account manager. Unless specifically indicated via contract, software license agreement, or other formal assignation, LSCPA Information Technology Services will serve as the account manager.

6.3.2.3. The information owner and IRM will establish conditions for group and role membership.

6.3.2.4. All accounts must be associated with an identifiable individual or a group of individuals, with compensating controls approved by the Information Security Officer (ISO), who are authorized to use the account, its group and role memberships, and access authorizations.

6.3.2.5. Accounts created must match the designated user's role and have approval from the information owner.

6.3.2.6. Information system accounts must be created, enabled, modified, disabled, and removed in accordance with LSCPA access control procedures.

6.3.2.7. Use of information system accounts must be monitored.

6.3.2.8. The information system account manager must update/revoke accounts:

6.3.2.8.1. when the accounts are no longer required,

6.3.2.8.2. when users are terminated or transferred, or

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

6.3.2.9. The information owner must authorize access 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. The information owner must review accounts at least annually to ensure their status is correct.

6.3.2.11. The IRM must establish a procedure for reissuing shared/group account credentials when individuals are removed from the group.

6.3.3. Access Enforcement (AC-3)

6.3.3.1. LSCPA information systems must enforce approved authorizations for logical access to information and information system resources in accordance with their approved information system security plans.

6.3.4. Separation of Duties (AC-5)

6.3.4.1. LSCPA will implement separation of duties for information system users.

6.3.4.2. Information owners must identify business requirements for separation of duties and document the requirements.

6.3.4.3. Information owners are required to consider separation of duties when approving access.

6.3.5. Least Privilege (AC-6)

6.3.5.1. Information owners must employ the principle of least privilege, only allowing accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with LSCPA missions and business functions.

6.3.6. Unsuccessful Logon Attempts (AC-7)

6.3.6.1. Information systems must limit consecutive invalid or unsuccessful logon attempts during a certain period of time. The IRM is responsible for determining the number of invalid logon attempts and the time period allowed.

6.3.6.2. Information systems must automatically lock the user account for a certain period of time when the maximum number of consecutive invalid or unsuccessful logon attempts is exceeded. The IRM is responsible for determining the period of time the account will remain locked.

6.3.7. System Use Notification (AC-8)

6.3.7.1. Information systems, where possible, must display an approved system use notification message or banner before granting access to the system that

provides privacy and security notices consistent with applicable laws and policies and that states:

6.3.7.1.1. Users are accessing a state-owned information system.

6.3.7.1.2. Usage may be monitored, recorded, and subject to audit.

6.3.7.1.3. Unauthorized use of the information system is prohibited and is subject to criminal prosecution and civil penalties.

6.3.7.1.4. Use of the information system indicates consent to monitoring and recording.

6.3.7.2. Information systems, where possible, must retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

6.3.7.3. For publicly accessible systems that require authentication:

6.3.7.3.1. The system displays use information before granting further access.

6.3.7.3.2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

6.3.7.3.3. Includes a description of the authorized uses of the system.

6.3.8. Permitted Actions Without Identification or Authentication (AC-14)

6.3.8.1. Information owners and information custodians must identify which user actions can be performed on an information system without identification or authentication, consistent with LSCPA mission and business functions.

6.3.8.2. User actions not requiring identification or authentication must be documented in the information system security plan, including supporting rationale.

6.3.9. Remote Access (AC-17)

6.3.9.1. The IRM and the ISO must establish and document usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access allowed.

6.3.9.2. The IRM and ISO must authorize remote access functionality to the information system prior to allowing such connections.

6.3.10. Wireless Access (AC-18)

6.3.10.1. The IRM and the ISO must establish and document usage restrictions, configuration and connection requirements, and implementation guidance for wireless access.

6.3.10.2. The IRM and ISO must authorize wireless access to the information system prior to allowing such connections.

6.3.10.3. Only personnel authorized by the IRM may configure wireless networks. Users must not install or configure wireless networks (including on printers, projectors, and other peripherals), ad hoc or otherwise, unless specifically authorized by the IRM in writing.

6.3.11. Access Control for Mobile Devices (AC-19)

6.3.11.1. The IRM and the ISO must establish and document usage restrictions, configuration requirements, and implementation guidance for LSCPA-controlled mobile devices.

6.3.11.2. The IRM and ISO must authorize the connection of mobile devices to LSCPA information systems.

6.3.12. Use of External Information Systems (AC-20)

6.3.12.1. The ISO and the information owner 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 LSCPA-controlled information using external information systems.

6.3.13. Publicly Accessible Content (AC-22)

6.3.13.1. The President designates personnel authorized to post information onto a publicly accessible information system, directly or by policy. (See Information Resources Policy 4.0 College Websites.)

6.3.13.2. The IRM and ISO will provide training to the designated personnel to ensure that publicly accessible information does not contain nonpublic information.

6.3.13.3. Designated personnel will review proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

6.3.13.4. Designated personnel will review the content on the publicly accessible information system for nonpublic information periodically based on risk and remove such information, if discovered.

6.4. Awareness and Training

6.4.1. Security Awareness and Training Policy and Procedures (AT-1)

6.4.1.1. LSCPA must provide an information security awareness program for all users of College information systems.

6.4.2. Security Awareness Training (AT-2)

6.4.2.1. The ISO must develop and implement a security awareness program to provide:

6.4.2.1.1. ongoing information security awareness training to all users;

6.4.2.1.2. a wide spectrum of information security training and awareness approaches;

6.4.2.1.3. online course training (certified by the Texas Department of Information Resources) for employees annually or as required by changes to security technologies;

6.4.2.1.4. new employees with an introduction to information security awareness and information security policies during the onboarding process;

6.4.2.1.5. formal acknowledgment by employees of LSCPA information security policies and procedures on an annual basis; and

6.4.2.1.6. information security awareness training requirements to contractors with access to LSCPA owned information systems or databases.

6.4.2.2. New employees must complete information security awareness within 30 days of hire.

6.4.2.3. All security awareness educational materials must be reviewed and updated on an annual basis and when triggered by relevant events such as information system changes that impact security, updates to security-related policies, and security incidents.

6.4.2.4. In addition to annual training requirements, employees may be assigned information security training by their unit heads, the ISO, or the IRM.

6.4.3. Role-Based Security Training (AT-3)

6.4.3.1. The ISO must provide role-based security training to groups whose members most often handle confidential and/or sensitive information (such as FERPA data and Personally Identifiable Information [PII]) or have administrative access to systems that store confidential and/or sensitive information.

6.4.3.2. Where possible, the user must complete the training before information owners authorize access to a system containing sensitive information.

6.4.4. Security Training Records (AT-4)

6.4.4.1. LSCPA must maintain:

6.4.4.1.1. security awareness and training documentation, and

6.4.4.1.2. security awareness and training records as per records retention requirements.

6.5. Audit and Accountability

6.5.1. Audit and Accountability Policy and Procedures (AU-1)

6.5.1.1. LSCPA must define purpose, scope, roles, responsibilities, and compliance requirements regarding audit.

6.5.1.2. LSCPA must monitor system logs for security and operational events including user access events that might lead to inappropriate access or impact to availability.

6.5.2. Audit Events (AU-2)

6.5.2.1. For all systems requiring authentication, the information system must audit events sufficiently to establish individual accountability for any action taken within the information system that affects the confidentiality, integrity, or availability of the system or information.

6.5.2.2. The information system should record connection, authentication, and access events as these are most pertinent to post-event investigations.

6.5.2.3. Audit logs of changes to mission-critical systems and security infrastructure must be maintained.

6.5.2.4. The information custodian must enhance the detail captured in audited events up to the capabilities of the information system as investigations reveal necessary changes.

6.5.3. Content of Records (AU-3)

6.5.3.1. Where possible, the information custodian must configure system audit records to include:

6.5.3.1.1. date/time of the event,

6.5.3.1.2. component of the information system where the event occurred,

6.5.3.1.3. description of event,

6.5.3.1.4. identity of subject/user, and

6.5.3.1.5. the outcome (success or failure) of the event.

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

6.5.4. Audit Storage Capacity (AU-4)

6.5.4.1. The auditing process must be protected by ensuring sufficient record storage capacity is available.

6.5.5. Response to Audit Processing Failures (AU-5)

6.5.5.1. Where possible, the information system must be configured to detect when logging has failed and report the failure to appropriate administrative personnel via automated alerting.

6.5.5.2. The information custodian must remediate logging discrepancies.

6.5.6. Audit Review, Analysis, and Reporting (AU-6)

6.5.6.1. System logs must be reviewed and analyzed for security and operational events (i.e., inappropriate activity, suspected violations, or unusual or otherwise suspicious activity) that might lead to inappropriate access or impact to availability. Responsibility and frequency must be documented in the information system security plan. This process may be automated.

6.5.6.2. The information custodian must investigate suspicious activity, take corrective action, or escalate to appropriate personnel on events identified during system log reviews or from automated alerting.

6.5.7. Time Stamps (AU-8)

6.5.7.1. The information custodians must synchronize LSCPA information systems with a pool of global clock sources.

6.5.7.2. Where possible, audit log entries must contain a date/time stamp using local synchronized time.

6.5.8. Protection of Audit Information (AU-9)

6.5.8.1. The information custodian must protect audit events and auditing tools against unauthorized access, modification, or deletion.

6.5.9. Audit Record Retention (AU-11)

6.5.9.1. The information custodian must retain audit records for a minimum of 30 days to provide a time sufficient to provide support after-the-fact security investigations and to meet relevant regulatory and records retention requirements.

6.5.10. Audit Generation (AU-12)

6.5.10.1. Where possible, the information systems must be configured to generate audit records containing information as required by policy.

6.5.10.2. LSCPA information systems must provide access control for recorded audit events.

6.6. Configuration Management

6.6.1. Configuration Management Policy and Procedures (CM-1)

6.6.1.1. LSCPA must utilize a configuration management program that effectively implements selected security controls and control enhancements as required by this policy. The program must be structured to prevent unauthorized or improper modifications to information system hardware, firmware, software, and documentation that considers the system risk posture, effect on College operations, and compliance with license agreements and intellectual property law.

6.6.2. Baseline Configuration (CM-2)

6.6.2.1. The information custodian must create a baseline configuration for each information system or groups of similar information systems.

6.6.2.2. The information custodian must ensure the baseline configuration stays current.

6.6.3. Security Impact Analysis (CM-4)

6.6.3.1. Proposed changes to an information system must be analyzed to determine potential security impacts prior to implementation. The information custodian is responsible for ensuring the analysis is performed.

6.6.3.2. Where possible, the changes must be analyzed on a separate test environment before implementation in an operational environment. Emergency changes to address high-risk vulnerabilities may be implemented directly to an operational environment.

6.6.3.3. The ISO and information owners must approve changes that affect security on information systems prior to implementation.

6.6.4. Configuration Settings (CM-6)

6.6.4.1. The information custodian and the ISO must establish, implement and document a mandatory minimally acceptable baseline of security settings for the major components of an information system using an agreed upon procedure and checklist that reflect the most restrictive security settings consistent with operational requirements and the system's risk posture.

6.6.4.2. The information custodian is responsible for implement the configuration settings.

6.6.4.3. The information custodian and the ISO must identify and document deviations from the established baseline security settings of the major components of information systems.

6.6.4.4. The information owner and the ISO must approve deviations from the established baseline security settings of the major components of information systems.

6.6.4.5. The information custodian must monitor and control changes to the baseline security settings of the major components of the information system in accordance with the established procedures for the system.

6.6.5. Least Functionality (CM-7)

6.6.5.1. The baseline configurations must ensure information system configurations provide only essential capabilities.

6.6.5.2. The information custodian must disable or restrict the use of those ports, services, and protocols within the information system deemed to be unnecessary or not secure.

6.6.6. Information System Component Inventory (CM-8)

6.6.6.1. The information custodian must document and maintain current inventory of information system components.

6.6.6.2. The inventory must include the information the information custodian deems necessary for tracking, reporting, and accountability (e.g., information owners).

6.6.6.3. The information custodian must review and update the inventory at least annually.

6.6.7. Software Usage Restrictions (CM-10)

6.6.7.1. Software and associated documentation must be used in accordance with contract agreements and copyright laws.

6.6.7.2. The IRM must track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

6.6.7.3. LSCPA must comply with intellectual property concerns, including peer-to-peer file sharing technologies as covered in the Higher Education Opportunity Act and other legislation and regulations, by blocking inappropriate use, taking corrective action, and documenting incidents.

6.6.7.4. When discovered, inappropriately licensed software must be removed from College-owned systems in a timely manner.

6.6.8. User Installed Software (CM-11)

6.6.8.1. The IRM must control installation of software on systems by users via the following processes:

6.6.8.1.1. The IRM must limit administrative access to desktop computers or computing instances to Information Technology Services or other approved personnel.

6.6.8.1.2. The IRM must monitor and enforce the limitation of administrative access to desktop computers or computing instances on a periodic basis.

6.7. Contingency Planning

6.7.1. Contingency Planning and Procedures (CP-1)

6.7.1.1. LSCPA must create, maintain, and distribute a plan for restoration of College information technology operations that addresses critical information systems to minimize the impact of any significant disruption to the mission and services they support.

6.7.1.2. LSCPA must implement procedures to facilitate information systems recovery planning.

6.7.2. Contingency Plan (CP-2, CP-10)

6.7.2.1. The IRM, with input from the ISO, must create and securely distribute the LSCPA IT Disaster Recovery Plan (DRP), which is informed by the LSCPA Continuity of Operations Plan. The DRP must:

6.7.2.1.1. Identify information systems and contingency requirements associated with essential missions and business functions identified in the LSCPA Continuity of Operations Plan.

6.7.2.1.2. Provide recovery objectives, restoration priorities, and metrics.

6.7.2.1.3. Address contingency roles, responsibilities, and assigned individuals with contact information.

6.7.2.1.4. Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

6.7.2.1.5. Address eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

6.7.2.1.6. Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

6.7.2.2. The IRM and ISO will coordinate contingency planning activities with incident handling activities (see Section 6.9 of this policy).

6.7.2.3. The DRP and any updates or changes will be distributed to key personnel identified in the plan.

6.7.2.4. The IRM and ISO will review and update the DRP annually, and also update it as necessary to address changes to the organization, information systems, or environment of operations and problems encountered during plan implementation, execution, or testing.

6.7.2.5. The DRP is designated as Confidential information and must be protected from unauthorized disclosure and modification.

6.7.3. Contingency Training (CP-3)

6.7.3.1. The IRM must provide training to users of information systems pertinent to their role in disaster recovery.

6.7.3.2. The IRM must conduct role-based training for employees within 30 days of assuming a role in disaster recovery, when there is a major change to the information system, and annually thereafter.

6.7.4. Contingency Plan Testing (CP-4)

6.7.4.1. The DRP must contain a provision for annual testing.

6.7.4.2. The IRM, information owner, and information custodian will review the results of the disaster recovery plan test and initiate corrective action if needed.

6.7.5. Alternate Storage Site (CP-6)

6.7.5.1. A copy of mission-critical College information system backup information must be stored at an alternate site that is geographically distinct from the information system location.

6.7.5.2. Information security controls at alternate site storage facilities must meet or exceed College information security controls including physical security and environmental control.

6.7.6. Information System Backup (CP-9)

6.7.6.1. User-level information on centralized information systems must be backed up at a frequency necessary to support the recovery time and recovery point objective identified for the system in the DRP.

6.7.6.2. System-level information on centralized information systems must be backed up at a frequency necessary to support the recovery time and recovery point objective identified for the system in the DRP.

6.7.6.3. System documentation, including security-related documentation, of centralized information systems must be backed up at a frequency necessary to support the recovery time and recovery point objective identified for the system in the DRP.

6.7.6.4. Backups must be protected at the same level as operational information, including physical security and access controls where the media is stored.

6.8. Identification and Authentication

6.8.1. Identification and Authentication Policy and Procedures (IA-1)

6.8.1.1. LSCPA must establish, implement, and maintain procedures for the implementation of the identification and authentication policy and associated identification and authentication controls.

6.8.1.2. The procedures must be reviewed on an annual basis and updated if necessary.

6.8.2. Identification and Authentication (Organizational Users) (IA-2)

6.8.2.1. Each user or process acting on behalf of a user must be assigned a unique identifier.

6.8.2.2. Multifactor authentication must be used where possible and compatible with LSCPA's approved multifactor authentication system(s).

6.8.3. Identifier Management (IA-4)

6.8.3.1. Issuance of Identifiers

6.8.3.1.1. LSCPA students (prospective, current, alumni) and employees are issued identifiers to be used throughout the course of their affiliation with the College.

6.8.3.1.2. Identifiers for groups/roles (i.e., shared accounts), or devices must be authorized by the IRM and relevant information owners and must be based on business need.

6.8.3.2. Selection of identifiers must be based on approved information system procedures.

6.8.3.3. Assigning and Reuse of Identifiers

6.8.3.3.1. Identifiers assigned to individuals must not be reused.

6.8.3.3.2. Re-use of identifiers for groups/roles (i.e., shared accounts) or devices must be based on business needs and authorized by the IRM.

6.8.3.4. Identifiers must be disabled upon the severance of the individual's relationship to the College. Exceptions may be made based on business need, with approval from the IRM and relevant information owners.

6.8.4. Authenticator Management (IA-5)

6.8.4.1. The identity of the individual, group, role, or device must be verified prior to receiving the authenticator (e.g., password, certificate, keycard, token).

6.8.4.2. The IRM must establish and implement requirements for authenticators to ensure they have sufficient strength of mechanism for their intended use.

6.8.4.3. The IRM must establish and implement procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

6.8.4.4. The information custodian must change factory-preset authenticators to meet College requirements prior to putting the system into production.

6.8.4.5. The IRM must establish and implement requirements for the minimum and maximum lifetime and reuse conditions for authenticators.

6.8.4.6. The IRM must establish and implement requirements for the changing or refreshing of authenticators.

6.8.4.7. Information systems must protect authenticator content from unauthorized disclosure and modification through hashing, encryption, or restricted access.

6.8.4.8. Individuals issued authenticators must keep them confidential, not share them, and report any suspected loss or exposure to the Information Technology Services department and the ISO.

6.8.4.9. Authenticators must be changed for group/role (i.e., shared) accounts when membership of those accounts changes.

6.8.4.10. Compromised authenticators must be reported to LSCPA's Information Technology Services department and/or the ISO immediately upon discovery.

6.8.4.11. Passwords

6.8.4.11.1. The IRM must establish standards for passwords including, but not limited to, password length, complexity, distribution, encryption, and reset. Passwords must be managed as per approved standards.

6.8.4.11.2. The IRM must establish and maintain procedures for the creation of initial password content that will be unique for each account and will meet the same complexity requirements as user-selected passwords.

6.8.4.12. The ISO must approve exceptions to minimum password requirements.

6.8.5. Authenticator Feedback (IA-6)

6.8.5.1. The information custodian must enable masking of password entry where possible to protect the content from possible use by unauthorized individuals.

6.8.6. Cryptographic Module Authentication (IA-7)

6.8.6.1. The IRM and ISO must approve implementation mechanisms for authentication to a cryptographic module that meet the requirements of all applicable federal and state laws.

6.8.7. Identification and Authentication (Non-Organizational Users) (IA-8)

6.8.7.1. Identifiers for non-LSCPA or third party (e.g., vendors, contractors, auditors, and consultants) users or processes must be authorized by the IRM and relevant information owners.

6.8.7.2. Identifiers assigned to third parties must be unique to that third party and not used or re-used by other third parties.

6.9. Incident Response

6.9.1. Incident Response Policy and Procedures (IR-1)

6.9.1.1. LSCPA must establish, implement, and maintain procedures for responding to an information security incident.

6.9.1.2. LSCPA must review and update its information security incident response procedures on an annual basis.

6.9.2. Incident Response Training (IR-2)

6.9.2.1. The IRM must provide training to personnel with incident response roles and responsibilities:

6.9.2.1.1. within 30 days of assuming an incident response role,

6.9.2.1.2. when relevant changes to an information system are made, and

6.9.2.1.3. annually thereafter.

6.9.3. Incident Handling (IR-4)

6.9.3.1. Security incidents must be assessed based on the business impact on the affected resources and the current and potential technical effect of the incident.

6.9.3.2. Security incidents will be designated as urgent incidents and subject to urgent incident reporting (see Section 6.9.5.5 of this policy) if one or more of the following criteria are met:

6.9.3.2.1. The incident has or may propagate to other state systems.

6.9.3.2.2. The incident will result in criminal violations required to be reported to law enforcement.

6.9.3.2.3. The incident involves the unauthorized disclosure or modification of confidential information.

6.9.3.3. The IRM and the ISO must develop and maintain an incident handling capability that includes preparation, detection and analysis, containment, eradication, and recovery. This may include the use of qualified external resources (e.g., from other system components, DIR, or vendors).

6.9.3.4. The IRM and ISO must coordinate incident handling activities with contingency planning activities (see Section 6.7 of this policy).

6.9.3.5. The IRM and ISO must incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing.

6.9.4. Incident Monitoring (IR-5)

6.9.4.1. The ISO must track and document information system security incidents.

6.9.5. Incident Reporting (IR-6)

6.9.5.1. All users of LSCPA information systems are required to report security incidents to their immediate supervisor, the Information Technology Services department, and the ISO in a prompt manner.

6.9.5.2. The ISO must be notified of any suspected data breaches (any incident in which Sensitive, Confidential, Regulated or otherwise protected data in human or machine-readable form is put at risk because of exposure to unauthorized individuals) within 48 hours of discovery.

6.9.5.3. Incidents involving information security must be managed by the ISO.

6.9.5.4. LSPCA must report security incidents as required by federal or state law or regulation.

6.9.5.5. Urgent Incident Reports

6.9.5.5.1. The ISO must promptly report any security incidents designated as urgent incidents to the Texas Department of Information Resources.

6.9.5.5.2. If the assessment of the security incident reveals suspected criminal activity, LSCPA will report the incident to law enforcement. The security incident will then be investigated, reported, and documented in accordance with the legal requirements for handling of evidence.

6.9.5.5.3. The ISO must report significant security incidents even if incomplete information is available and must continue to report information as it is collected.

6.9.5.5.4. Monthly Incident Reports, to include summary reports of security-related incidents for that month, must be sent to the Texas Department of Information Resources no later than nine (9) calendar days after the end of the month.

6.9.5.6. The Contracts Manager must ensure vendor security incident reporting requirements are included in contracts.

6.9.6. Incident Response Assistance (IR-7)

6.9.6.1. The IRM and ISO must provide advice and assistance resources to the users of LSCPA information systems for the handling and reporting of security incidents.

6.9.7. Incident Response Plan (IR-8)

6.9.7.1. The IRM and ISO must create and distribute a security incident response plan that:

6.9.7.1.1. outlines incident response within the College;

6.9.7.1.2. describes the structure and organization of the incident response capability;

6.9.7.1.3. provides a high-level approach for how the incident response capability fits into the overall organization;

6.9.7.1.4. meets the unique requirements of the College;

6.9.7.1.5. defines which incidents must be reported and handled as security incidents;

6.9.7.1.6. defines metrics to monitor effectiveness;

6.9.7.1.7. defines resources and management support needed to maintain and mature incident response capability; and

6.9.7.1.8. is reviewed and approved by executive management.

6.9.7.2. The incident response plan must be distributed to appropriate key personnel as defined in the plan and executive management.

6.9.7.3. The IRM and ISO must review the incident response plan annually and update the incident response plan annually or as required to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

6.9.7.4. Communicates incident response plan changes to key personnel as defined in the plan and executive management.

6.9.7.5. The incident response plan must be protected from unauthorized disclosure and modification.

6.10. Maintenance

6.10.1. Maintenance Policy and Procedures (MA-1)

6.10.1.1. LSCPA must establish, implement, and maintain procedures to ensure that maintenance of information systems is performed in a secure manner.

6.10.1.2. LSCPA must review and update its information system maintenance procedures on an annual basis.

6.10.2. Controlled Maintenance (MA-2)

6.10.2.1. The information custodian must schedule, perform, document and review records of maintenance and repairs on information systems in accordance with manufacturer or vendor recommendations or LSCPA requirements.

6.10.2.2. The information owner and information custodian must approve and monitor all maintenance activities whether performed on site or remotely and whether equipment is serviced on site or removed to another location.

6.10.2.3. The information owner and information custodian must approve removal of an information system or system components from LSCPA facilities for off-site maintenance or repairs.

6.10.2.4. The information custodian must sanitize equipment to remove all information from associated media prior to removal from LSCPA facilities for off-site maintenance or repairs.

6.10.2.5. The information custodian must check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

6.10.2.6. The information custodian must retain maintenance information and records of activities performed on information systems.

6.10.3. Nonlocal Maintenance (MA-4)

6.10.3.1. The information custodian must approve, monitor, and document nonlocal information system maintenance activities.

6.10.3.2. The use of nonlocal maintenance and diagnostic tools must be consistent with the information system security plan.

6.10.3.3. Strong authentication methods must be used when establishing nonlocal maintenance and diagnostic sessions.

6.10.3.4. Sessions and network connections must be terminated when nonlocal maintenance is completed.

6.10.4. Maintenance Personnel (MA-5)

6.10.4.1. The information custodian must establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

6.10.4.2. The information custodian must ensure that non-escorted personnel performing maintenance on an information system have the required access authorizations.

6.10.4.3. The information custodian must ensure that LSCPA personnel with the required access authorizations and technical competence are available to

supervise the maintenance activities of personnel who do not possess the required access authorizations.

6.11. Media Protection

6.11.1. Media Protection Policy and Procedures (MP-1)

6.11.1.1. LSCPA must establish, implement, and maintain procedures for the secure use, storage, and transportation of storage media containing sensitive information.

6.11.1.2. LSCPA must review and update its media protection procedures on an annual basis.

6.11.2. Media Access (MP-2)

6.11.2.1. The information custodian must restrict access to digital and non-digital media containing Confidential, Sensitive, Regulated, or Mission Critical information to authorized individuals.

6.11.2.2. Lost or stolen digital and non-digital media, regardless of ownership, that contains College data must be reported to the Information Technology Services department and/or the ISO immediately.

6.11.3. Media Sanitization (MP-6)

6.11.3.1. Prior to disposal or transfer, the information custodian must ensure media that contains sensitive information is securely sanitized (erased or destroyed) in a manner that ensures the information cannot be recovered or reconstructed.

6.11.3.2. The information custodian must ensure that electronic media (e.g., internal to computers, MFPs, and removable media) is either shredded or securely erased with tools approved by the ISO and commensurate with the security category of the information.

6.11.3.3. The information custodian must keep documentation of erasure or destruction that describes the process and sanitization tools used to remove the information or destroy the digital media.

6.11.3.4. Hard copies of Sensitive, Confidential, or Regulated information must be shredded securely before disposal.

6.11.4. Media Use (MP-7)

6.11.4.1. LSCPA may restrict the use of removable, external, or portable media (e.g., CDs, DVDs, external hard drives, flash drives, thumb drives, or other portable storage devices) on certain information systems that store or process Sensitive, Confidential, or Regulated information.

6.11.4.2. The information custodian must develop and maintain procedures to enforce any restrictions on removable, external, or portable media.

6.12. Physical and Environmental Protection

6.12.1. Physical and Environmental Protection Policy and Procedures (PE-1)

6.12.1.1. LSCPA must ensure that areas containing critical technology infrastructure (CTI) are protected by appropriate physical and environmental protection controls and procedures. CTI areas include, but are not limited to, data

centers, server rooms, and areas housing network and communications equipment.

6.12.1.2. The IRM and Director of Physical Plant must develop, document, and manage physical and environmental protection controls and procedures for CTI areas.

6.12.1.3. LSCPA must review physical and environmental protection controls and procedures protecting CTI areas on a schedule consistent with risk posture based on:

6.12.1.3.1. the security categorization of information systems housed in or dependent upon the CTI areas (see Section 6.13 of this policy);

6.12.1.3.2. the value of equipment housed in CTI areas; and

6.12.1.3.3. the criticality of non-CTI equipment (e.g., electrical and mechanical) housed in CTI areas.

6.12.1.4. Only authorized equipment will be placed or installed in CTI areas. CTI areas must not be used as storage locations for unrelated items (e.g., office supplies, furniture, janitorial supplies).

6.12.2. Physical Access Authorizations (PE-2)

6.12.2.1. Access to CTI areas must be authorized by the IRM and be granted only to those individuals requiring access for operational or maintenance duties.

6.12.2.2. The IRM and Director of Physical Plant must maintain and keep current a list of personnel with authorized access to CTI areas.

6.12.2.3. LSCPA must issue authorization credentials allowing access to CTI areas.

6.12.2.4. Access to CTI areas must be reviewed annually, or more frequently based on risk posture.

6.12.2.5. Credentials allowing access to CTI areas must be recovered when access is no longer required.

6.12.3. Physical Access Control (PE-3, PE-8)

6.12.3.1. Physical access points to CTI areas must be controlled using appropriate physical security controls based on risk posture.

6.12.3.2. Individual authorizations to CTI areas must be verified before each access is granted.

6.12.3.3. Physical access audit logs (including visitor access) for CTI areas must be retained by Information Technology Services for a minimum of 30 days.

6.12.3.4. No CTI areas will be designated as publicly accessible.

6.12.3.5. Visitors to CTI areas must be escorted and monitored.

6.12.3.6. Physical access devices (e.g., keys, access cards, combinations) for CTI areas must be:

6.12.3.6.1. stored and assigned in a secure manner;

6.12.3.6.2. inventoried annually, or more frequently based on risk posture;

6.12.3.6.3. recovered from individuals whose access has been rescinded;

6.12.3.6.4. changed when lost or compromised; and

6.12.3.6.5. changed, in the case of Personal Identification Numbers (PINs) and combinations, when known by an individual whose access has been rescinded and periodically based on risk posture.

6.12.3.7. Lost or stolen credentials and physical access devices must be reported immediately to the IRM, ISO, Director of Physical Plant, and Campus Security.

6.12.4. Monitoring Physical Access (PE-6, PE-8)

6.12.4.1. Physical access to CTI areas must be monitored to detect and respond to physical security incidents.

6.12.4.2. Physical access logs (including visitor access) to CTI areas must be reviewed by the IRM (or designee) monthly, or more frequently based on risk posture.

6.12.4.3. Unauthorized or suspicious access and unusual events or incidents related to physical access to CTI areas must be treated as potential security incidents (see Section 6.9 of this policy) and reported to the IRM, ISO, and Director of Physical Plant.

6.12.5. Emergency Power (PE-11)

6.12.5.1. LSCPA must provide short-term power via uninterrupted power supply (UPS) or via generator to critical technology infrastructure to facilitate orderly shutdown or transition to alternate power in the event of a primary power loss.

6.12.5.2. Alternate power solutions should be based on the College's Business Continuity Plan.

6.12.6. Emergency Lighting (PE-12)

6.12.6.1. The College's data center room and server rooms must have emergency lighting that covers emergency exits that activates in the event of a power outage or disruption.

6.12.7. Fire Protection (PE-13)

6.12.7.1. Fire detection and suppression systems or devices using an independent power source will be employed and maintained inside all CTI areas, where possible and practical.

6.12.8. Temperature and Humidity Controls (PE-14)

6.12.8.1. Humidity and temperature for CTI areas must be monitored and maintained within acceptable levels based on equipment specifications.

6.12.9. Water Damage Protection (PE-15)

6.12.9.1. LSCPA must prevent water damage to certain designated critical technology infrastructure by providing an emergency water shutoff mechanism that is working properly, regularly tested and known to key personnel.

6.12.10. Delivery and Removal (PE-16)

6.12.10.1. Delivery and removal of critical technology infrastructure components (e.g., servers, network equipment, telephony equipment) to and from CTI areas must be authorized by the IRM (or designee) and documented.

6.13. Risk Assessment

6.13.1. Risk Assessment Policy and Procedures (RA-1)

6.13.1.1. LSCPA must establish, implement, and maintain procedures for a risk management program that directs the completion of risk assessments on information systems including identifying, evaluating and documenting the level of impact of actualization of those risks.

6.13.1.2. LSCPA must review the risk management program at least annually as part of the Information Security Program annual review. (See Information Resources Policy 5.0 Information Security Program.)

6.13.2. Security Categorization (RA-2)

6.13.2.1. The information owner must categorize the information and the information system using the College's data classification standard and in accordance with applicable laws, regulations, and polices. (See Information Resources Policy 5.0 Information Security Program, Section 5.5.)

6.13.2.2. The ISO and information owners must document the security categorization results including supporting rationale in the security plan for the information system. (See Section 6.18 of this policy.)

6.13.3. Risk Assessment (RA-3)

6.13.3.1. The information owner and information custodian must complete (or commission for completion) and document an assessment of risk.

6.13.3.1.1. The risk assessment must include likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

6.13.3.1.2. Each identified risk must be assigned a ranking of High, Moderate, or Low.

6.13.3.1.3. The risk assessment results must be documented in a written report and protected from unauthorized disclosure, modification, or destruction.

6.13.3.1.4. The risk assessment results must be documented in the security plan for the information system. (See Section 6.18 of this policy.)

6.13.3.2. Risk assessment results must be reviewed and disseminated as per the College’s information security risk management process. (See Information Resources Policy 5.0 Information Security Program, Section 5.6.)

6.13.3.3. The frequency of risk assessments will be based on the security category of information and information systems being assessed and by certain triggering events:

6.13.3.3.1. Information and information systems with a security categorization of high must be assessed annually.

6.13.3.3.2. Information and information systems with a security categorization of low or moderate must be assessed biennially, at a minimum.

6.13.3.3.3. Certain information systems may require more frequent assessments, as directed by the ISO.

6.13.3.3.4. Risk assessments must be updated if there is a significant change to the information system or environment of operations, or other conditions that may impact the security state of the system.

6.13.3.3.5. The ISO may require completion of a full or partial risk assessment of an information system outside of the normal assessment cycle in response to a security incident.

6.13.4. Vulnerability Scanning (RA-5)

6.13.4.1. The information custodian must conduct vulnerability scans at least annually or when significant new vulnerabilities affecting an information system are identified and reported.

6.13.4.2. The ISO may conduct additional vulnerability scans at their discretion.

6.13.4.3. The vulnerability scanning tools and techniques will facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

6.13.4.3.1. enumerating platforms, software flaws, and improper configurations;

6.13.4.3.2. formatting checklists and test procedures; and

6.13.4.3.3. measuring vulnerability impact.

6.13.4.4. Vulnerability scan reports and results from security control assessments must be analyzed.

6.13.4.5. The information custodian remediates legitimate vulnerabilities in accordance with an organizational assessment of risk.

6.13.4.6. Information obtained from the vulnerability scanning process and security control assessments performed on information systems for which the College has custodial responsibility must be shared with the IRM, ISO, and relevant information custodians to help eliminate similar vulnerabilities in other information systems.

6.14. Security Assessment and Authorization

6.14.1. Security Assessment and Authorization Policy and Procedures (CA-1)

6.14.1.1. LSCPA's Information Security Program must assess and enhance the information security posture of the College through use of security assessment and risk assessment (see Section 6.13 of this policy) processes.

6.14.1.2. LSCPA will develop procedures to facilitate the security assessment and risk assessment processes.

6.14.2. Security Assessments (CA-2)

6.14.2.1. The ISO and the information custodian must develop a security assessment plan that describes the scope of the assessment including:

6.14.2.1.1. security controls and control enhancements under assessment;

6.14.2.1.2. assessment procedures to be used to determine security control effectiveness; and

6.14.2.1.3. the assessment environment, assessment team, and assessment roles and responsibilities

6.14.2.2. The ISO and the information custodian must assess the security controls in the information system and its environment of operations annually or as documented in the information system's security plan to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcomes.

6.14.2.3. The ISO must produce a security assessment report that documents the results of the assessment to be provided to the information owner, IRM, and authorizing official.

6.14.3. System Interconnections (CA-3)

6.14.3.1. The ISO, IRM and authorizing official must authorize all dedicated, non-transitory connections from College information systems to non-College information systems through the use of an interconnection security agreement.

6.14.3.2. The interconnection security agreement must document the interface characteristics, security requirements, and nature of the information communicated for each system interconnection.

6.14.3.3. LSCPA may use contracts as interconnection security agreements to ensure security controls of external parties are the same or better than local security controls.

6.14.3.4. The ISO and IRM must review the interconnection security agreements annually or prior to contract renewal.

6.14.4. Plan of Action and Milestones (CA-5)

6.14.4.1. The ISO must develop a plan of action and milestones for the information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system.

6.14.4.2. The ISO must update the plan of action and milestones annually or based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

6.14.5. Security Authorization (CA-6)

6.14.5.1. The authorizing official, IRM, and information owner must approve an information system for processing before it is moved into production or when a significant change is made.

6.14.5.2. The authorizing official, IRM, and information owner must approve the security posture of an information system.

6.14.5.3. The authorizing official, IRM, and information owner will update the security authorization annually except for systems with continuous monitoring programs in place. A continuous monitoring program will satisfy the annual security authorization update.

6.14.6. Continuous Monitoring (CA-7)

6.14.6.1. For each information system or group of related information systems, the ISO and the information custodian(s) must develop a continuous monitoring program that includes:

6.14.6.1.1. The establishment of security metrics to be monitored based on the information system or group of systems.

6.14.6.1.2. The establishment of periodic monitoring and assessment of information system controls on a schedule consistent with system risk.

6.14.6.1.3. Procedures for ongoing security status monitoring of the security metrics established by the ISO and information custodian.

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

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

6.14.6.1.6. Required security reporting. (See Information Resources Policy 5.0 Information Security Program, Section 5.8.)

6.14.7. Internal System Connections (CA-9)

6.14.7.1. Internal connections between information systems and system components (e.g., printers, copiers, computers, mobile devices, etc.) must be authorized.

6.14.7.2. The IRM and ISO must develop and maintain standards for LSCPA-approved connections between information system components or classes of components. Standards must include interface characteristics, security requirements, and the authorized nature of the information communicated.

6.14.7.3. Requests for connections that are not pre-approved must be submitted and approved through LSCPA's IT work order system.

6.15. System and Communications Protection

6.15.1. System and Communications Protection Policy and Procedures (SC-1)

6.15.1.1. LSCPA must establish, implement, and maintain procedures for ensuring the protection of internal and external information system communications.

6.15.1.2. LSCPA must review and, if necessary, update the information system communication procedures on an annual basis.

6.15.2. Denial of Service Protection (SC-5)

6.15.2.1. The IRM, in collaboration with the ISO, must establish, implement, and maintain procedures to protect against or limit the effects of various types of denial of service attacks against on-campus mission critical information systems or critical network infrastructure.

6.15.3. Boundary Protection (SC-7)

6.15.3.1. Communications must be monitored and controlled at external boundaries of information systems and at key internal boundaries within the information system.

6.15.3.2. Subnetworks that are logically separated from internal networks must be implemented for publicly accessible system components.

6.15.3.3. Information systems must connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with LSCPA security architecture.

6.15.4. Transmission Confidentiality and Integrity (SC-8)

6.15.4.1. The information system must protect the confidentiality and integrity of transmitted information through the use of protected distribution systems and/or the use of encryption.

6.15.5. Cryptographic Key Establishment and Management (SC-12)

6.15.5.1. Where possible, the IRM and information custodian must establish, implement, and maintain procedures for managing the cryptographic keys required for cryptography employed within information systems.

6.15.6. Cryptographic Protection (SC-13)

6.15.6.1. The IRM and the ISO must establish, implement, and maintain procedures for the use of cryptographic technologies and tools to protect College information and information systems in accordance with applicable laws and policies.

6.15.7. Collaborative Computing Devices (SC-15)

6.15.7.1. Remote activation of collaborative computing devices (e.g. network whiteboards, cameras, microphones) is prohibited, except where specifically permitted by the IRM.

6.15.7.2. Where possible, the devices should provide an explicit indication of use to users physically present at the device.

6.15.8. Voice Over Internet Protocol (SC-19)

6.15.8.1. LSCPA must establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to information systems if used maliciously.

6.15.8.2. The Information Technology Services department must authorize, monitor and control the use of VoIP within the College network.

6.15.9. Secure Name/Address Resolution Service (Authoritative Source) (SC-20)

6.15.9.1. The name resolution system(s) must be configured to provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

6.15.9.2. The name resolution system(s) must be configured to provide 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.

6.15.10. Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)

6.15.10.1. Where possible, information systems must be configured to request and perform data origin authentication and data integrity verification on the

name/address resolution responses the system receives from authoritative sources.

6.15.11. Architecture and Provisioning for Name/Address Resolution Service (SC-22)

6.15.11.1. Information systems that collectively provide name/address resolution service for LSCPA must be fault-tolerant and implement internal/external role separation.

6.15.12. Process Isolation (SC-39)

6.15.12.1. Where possible, LSCPA must specify and configure information systems that maintain a separate execution domain for each executing process.

6.16. System and Information Integrity

6.16.1. System and Information Integrity Policy and Procedures (SI-1)

6.16.1.1. LSCPA must establish, implement, and maintain procedures to protect the integrity of information systems and the information they contain.

6.16.1.2. LSCPA must review and update the procedures on an annual basis.

6.16.2. Flaw Remediation (SI-2)

6.16.2.1. Information custodians and key users of mission critical or high value systems must participate in the identification, reporting, and/or correction of information system flaws.

6.16.2.2. For mission critical or high value systems, the information custodian must test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

6.16.2.3. The information custodian must install security-relevant software and firmware updates within a timeframe appropriate for the system and the type of update being installed.

6.16.2.4. LSCPA must incorporate flaw remediation into its organizational configuration management process.

6.16.3. Malicious Code Protection (SI-3)

6.16.3.1. LSCPA must employ malicious code protections on information systems and at other locations on the network based on system risk posture.

6.16.3.2. The information custodian must update malicious code protection mechanisms whenever new releases are available in accordance with LSCPA configuration management policy and procedure.

6.16.3.3. Malicious code protection mechanisms must be configured to:

6.16.3.3.1. Perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with LSCPA security policy.

6.16.3.3.2. Send alerts to the information custodians or system administrators in response to malicious code detections.

6.16.3.4. LSCPA must address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

6.16.4. Information System Monitoring (SI-4)

6.16.4.1. The information custodian must monitor information systems to detect:

6.16.4.1.1. Attacks and indicators of potential attacks

6.16.4.1.2. Unauthorized local, network, and remote connections

6.16.4.2. The information custodian, in collaboration with the IRM and ISO, will identify unauthorized use of the information system through the use of various monitoring tools and techniques.

6.16.4.3. The information custodian, in collaboration with the IRM and ISO, will deploy monitoring devices:

6.16.4.3.1. Strategically within the information system to collect information deemed essential.

6.16.4.3.2. At ad hoc locations within the system to track specific types of transactions of interest.

6.16.4.4. Information obtained from intrusion-monitoring tools must be protected from unauthorized access, modification, and deletion.

6.16.4.5. The level of information system monitoring will be increased in response to indications of increased risk to LSCPA operations and assets, individuals, other organizations, or the nation based on law enforcement or other credible sources of information.

6.16.4.6. LSCPA will obtain legal opinion as warranted with regards to information system monitoring activities in accordance with federal law, Texas law, or Texas State University System policies.

6.16.4.7. The IRM, ISO, or information custodian must provide monitoring information to the information owner or executive management upon request.

6.16.5. Security Alerts, Advisories, and Directives

6.16.5.1. The IRM and ISO must receive information system security alerts, advisories, and directives from various external organizations (e.g., MS-ISAC, vendors, or media) on an ongoing basis.

6.16.5.2. The IRM and ISO must generate internal security alerts, advisories, and directives as deemed necessary.

6.16.5.3. The IRM or ISO will disseminate security alerts, advisories, and directives to the appropriate internal or external personnel.

6.16.6. Information Handling and Retention (SI-12)

6.16.6.1. Both information within the information system and information output from the system must be handled and retained in accordance with applicable laws and record retention requirements.

6.17. System and Services Acquisition

6.17.1. System and Services Acquisition Policy and Procedures (SA-1)

6.17.1.1. LSCPA must establish, implement, and maintain procedures for identifying, documenting, and addressing security requirements during all phases of information system development or acquisition.

6.17.1.2. LSCPA must review and update the procedures on an annual basis.

6.17.2. Allocation of Resources (SA-2)

6.17.2.1. The IRM, ISO, and information owner must determine the information security requirements for an information system or information system service in mission or business process planning.

6.17.2.2. LSCPA must allocate the resources required to protect the information system or information system service as part of its approach to selecting, managing, and evaluating information technology.

6.17.2.3. LSCPA must establish a discrete budgetary line item for information security.

6.17.3. System Development Lifecycle (SA-3)

6.17.3.1. The information system must be managed using an appropriate information system development life cycle that incorporates information security considerations.

6.17.3.2. The information owner and information custodian must define and document information security roles and responsibilities throughout the system development lifecycle.

6.17.3.3. Individuals having information security roles and responsibilities must be included in development.

6.17.3.4. The College's information security risk management process must be integrated into system development life cycle activities.

6.17.4. Acquisition Process (SA-4)

6.17.4.1. The IRM and ISO must, in cooperation with the Director of Purchasing and Contracts, establish and maintain procedures for giving the appropriate level of consideration to the following requirements, descriptions, and criteria, explicitly or by reference, when acquiring information systems, system components, or information system services:

6.17.4.1.1. security functional requirements;

6.17.4.1.2. security strength requirements;

6.17.4.1.3. security assurance requirements;

6.17.4.1.4. security-related documentation requirements;

6.17.4.1.5. requirements for protecting security-related documentation;

6.17.4.1.6. description of the information system development environment and environment in which the system is intended to operate; and

6.17.4.1.7. acceptance criteria.

6.17.5. Information System Documentation (SA-5)

6.17.5.1. The IRM or information custodian, as appropriate, must obtain administrator documentation for the information system, system components, or information system service that describes:

6.17.5.1.1. secure configuration, installation, and operation of the system, component, or service;

6.17.5.1.2. effective use and maintenance of security functions or mechanisms; and

6.17.5.1.3. known vulnerabilities regarding configuration and uses of administrative functions.

6.17.5.2. The IRM or information custodian, as appropriate, must obtain user documentation for the information system, system component, or information system service that describes:

6.17.5.2.1. user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

6.17.5.2.2. methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

6.17.5.2.3. user responsibilities in maintaining the security of the system, component, or service.

6.17.5.3. The IRM or information custodian, as appropriate, must document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and inform the ISO and information owner of the results.

6.17.5.4. The IRM or information custodian, as appropriate, must protect the documentation as required, in accordance with the risk management strategy.

6.17.5.5. The IRM or information custodian, as appropriate, must distribute relevant documentation to information owners, information system administrators, and information system users as required.

6.17.6. External Information System Services (SA-9)

6.17.6.1. LSCPA must require that providers of external information system services comply with College information security requirements and employ College-defined security controls in accordance with applicable laws and policies.

6.17.6.2. The IRM and ISO, in collaboration with the Director of Purchasing and Contracts, must define and document appropriate oversight and user roles and responsibilities regarding external information system services.

6.17.6.3. LSCPA must monitor security control compliance by external service providers on an ongoing basis.

6.17.7. Developer Configuration Management (SA-10)

6.17.7.1. When LSCPA internally develops or contracts the development of an information system, system component, or information system service, LSCPA must require the developer to:

6.17.7.1.1. Perform configuration management during system, component, or service design, development, implementation, and/or operation as applicable.

6.17.7.1.2. Document, manage, and control the integrity of changes to the information system configuration and/or security controls.

6.17.7.1.3. Implement only LSCPA-approved changes to the system, component, or service.

6.17.7.1.4. Document approved changes to the system, component, or service and the potential security impacts of such changes.

6.17.7.1.5. Track security flaws and flaw resolution within the system, component, or service and report findings to the IRM.

6.18. System Security Planning

6.18.1. Security Planning Policy and Procedures (PL-1)

6.18.1.1. LSCPA must establish, implement, and maintain policy and procedures that address the effective implementation of selected security controls.

6.18.1.2. LSCPA must review and update its security planning policy and procedures on an annual basis.

6.18.2. System Security Plan (PL-2)

6.18.2.1. The information custodian, information owner, IRM and the ISO must develop and use a plan for each information system which:

6.18.2.1.1. is consistent with the College's enterprise architecture;

6.18.2.1.2. defines the authorization boundary for the system;

6.18.2.1.3. describes the operational context of the information system in terms of missions and business processes;

6.18.2.1.4. provides the security categorization of the information system including supporting rationale, based on classification of data stored, processed, or transmitted by the system and other relevant factors (see Section 6.13 of this policy);

6.18.2.1.5. describes the operational environment for the information system and relationships with or connections to other information system;

6.18.2.1.6. provides an overview of the security requirements for the system, including applicable legislative or regulatory requirements;

6.18.2.1.7. identifies any baseline configurations or templates used;

6.18.2.1.8. describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

6.18.2.1.9. must be approved by the ISO, the IRM, and appropriate information owners.

6.18.2.2. System security plans must be on file with the ISO. The ISO will distribute copies of the security plan and communicate subsequent changes to appropriate parties.

6.18.2.3. The security plan must be reviewed during subsequent risk assessments.

6.18.2.4. The plan must be updated to address changes to the information system, the operating environment, or problems found during implementation or risk assessments.

6.18.2.5. The plan must be protected from unauthorized disclosure and modification.

6.18.3. Rules of Behavior (PL-4)

6.18.3.1. LSCPA must establish and make available to users the rules that describe their responsibilities and expected behaviors with regards to information and information system usage in Information Resources Policy 2.0 Appropriate Use of Information Resources.

6.18.3.2. All employees, contractors, vendors, and other College-affiliated parties must formally acknowledge that they have read, understand, and agree to abide by the Information Resources Policy 2.0 Appropriate Use of Information Resources and the College's information security policies prior to being authorized to access College information and information systems.

6.18.3.3. LSCPA must review and update the Information Resources Policy 2.0 Appropriate Use of Information Resources as per the College's Information Resources policy review cycle.

6.18.3.4. Information owners must require individuals who have formally acknowledged a previous version of Information Resources Policy 2.0 Appropriate Use of Information Resources to read and re-acknowledge when Information Resources Policy 2.0 Appropriate Use of Information Resources is revised or updated.

6.19. Exceptions

6.19.1. An exception from this policy may be granted under certain circumstances. Exception requests shall be submitted in the manner set forth in Information Resources Policy 5.0 Information Security Program.

6.20. Related Policies, Regulations, Standards, and Guidelines

6.20.1. Texas DIR Security Control Standards Catalog

6.20.2. 1 Tex. Admin. Code §202.76

6.20.3. LSCPA Information Resources Policy 1.0 Information Resources Management

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

6.20.5. LSCPA Information Resources Policy 4.0 College Websites

6.20.6. LSCPA Information Resources Policy 5.0 Information Security Program

APPENDICES

APPENDIX A: Acronyms

APPENDIX B: Glossary

APPENDIX C: Website Accessibility Statement

APPENDIX D: Linking Notice

APPENDIX E: Website Privacy Notice

APPENDIX A: Acronyms

BCC.....Business and Commerce Code

CTI.....Critical Technology Infrastructure

CNSSI .....Committee on National Security Systems Instruction

DIR .....Department of Information Resources

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

NISTIR.....National Institute of Standards and Technology Interagency or Internal Report

PII .....Personal Identifying Information, Personally Identifiable Information

PIN .....Personal Identification Number

SP.....Special Publication

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. [1 Tex. Admin. Code §202.1(1)]

Access Control - The process of granting or denying specific requests to obtain and use information and related information processing services and to enter specific physical facilities. [FIPS 201-2, adapted]

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. [1 Tex. Admin. Code §213.1(1)]

Account - A mechanism relating to identity that provides access to an information system or network.

Administrative Access - Privileged access that bypasses user-level controls in order to manage the information system.

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. [1 Tex. Admin. Code §213.1(2)]

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. [1 Tex. Admin. Code §213.1(3)]

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. [1 Tex. Admin. Code §213.1(4)]

Audit Log - A chronological record of information system activities, including records of system accesses and operations performed in a given period. [CNSSI 4009]

Audit Record - An individual entry in an audit log related to an audited event. [NIST SP 800-53 Rev 4]

Authentication - Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to information resources. [FIPS 200, adapted]

Authenticator - The means used to confirm the identity of a user, processor, or device (e.g., user password or token). [NIST SP 800-53 Rev 4]

Authorization - The official management decision to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, based on the implementation of an agreed-upon set of security controls. [NIST SP 800-53 Rev 4, adapted]

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. [NIST SP 800-53 Rev 4]

Authorizing Official - A senior or executive manager with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations. [NIST SP 800-53 Rev 4, adapted]

Availability - The security objective of ensuring timely and reliable access to and use of information. [1 Tex. Admin. Code §202.1(3)]

Backup - A copy of files and programs made to facilitate recovery, if necessary. [NIST SP 800-34 Rev 1]

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 [NIST SP 800-53 Rev 4]

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. [NIST SP 800-53 Rev 4]

Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. [NIST SP 800-34 Rev 1]

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.

Compensating Security Controls - The security controls employed in lieu of the recommended controls that provide equivalent or comparable protection. [NIST SP 800-53 Rev 4, adapted]

Confidential Information - Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. [1 Tex. Admin. Code §202.1(5)]

Confidentiality - The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [1 Tex. Admin. Code §202.1(6)]

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. [NIST SP 800-53 Rev 4]

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. [NIST SP 800-53 Rev 4]

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.

Control - A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [1 Tex. Admin. Code §202.1(7)]

Critical Technology Infrastructure (CTI) - Information technology infrastructure (e.g., servers, networking equipment, telephony equipment) which supports mission critical business functions or services.

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. [1 Tex. Admin. Code §202.1(11)]

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. [NIST SP 800-53 Rev 4]

Digital Media - A form of electronic media where data are stored in digital (as opposed to analog) form. [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. [NIST SP 800-34 Rev 1, adapted]

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. [CNSSI 4009]

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. [1 Tex. Admin. Code §213.1(6)]

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. [1 Tex. Admin. Code §213.1(5)]

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. [1 Tex. Admin. Code §202.1(13)]

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. [44 U.S.C. Sec. 3601]

Event - Any observable occurrence in an information system. [NIST SP 800-53 Rev 4]

External Information System (or Component) - An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [NIST SP 800-53 Rev 4]

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. [NIST SP 800-53 Rev 4]

External Network - A network not controlled by the organization. [NIST SP 800-53 Rev 4]

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. [CNSSI 4009]

Guideline - Recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. [1 Tex. Admin. Code §202.1(14)]

Hardware - The physical components of an information system. [CNSSI 4009]

Home Page - The initial page that serves as the front door or entry point to a state website. [1 Tex. Admin. Code §206.1(12)]

Identifier - Unique data used to represent a person's identity and associated attributes. [FIPS 201-2, adapted]

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. [NIST SP 800-53 Rev 4, adapted]

Incident - See Security Incident.

Information - Data as processed, stored, or transmitted by a computer. [1 Tex. Admin. Code §202.1(16)]

Information Custodian - A department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource. [1 Tex. Admin. Code §202.1(17)]

Information Owner - A person with statutory or operational authority for specified information or information resources. [1 Tex. Admin. Code §202.1(18)]

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. [TGC §2054.003(7)]

Information Resources Manager - 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. [44 U.S.C., Sec. 3542]

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. [1 Tex. Admin. Code §202.1(21)]

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. [NIST SP 800-53 Rev 4, adapted]

Information System - An interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications and people. [1 Tex. Admin. Code §202.1(22)]

Information System Component - A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products. [NIST SP 800-53 Rev 4]

Information System Service - A capability provided by an information system that facilitates information processing, storage, or transmission. [NIST SP 800-53 Rev 4]

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. [1 Tex. Admin. Code §213.9]

Integrity - The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. [1 Tex. Admin. Code §202.1(23)]

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. [CNSSI 4009]

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. [NIST SP 800-53 Rev 4]

Internet - An electronic communications network that connects computer networks and computer facilities around the world. [1 Tex. Admin. Code §206.1(14)]

Local Access - Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. [NIST SP 800-53 Rev 4]

Malicious Code - 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 malicious code. [NIST SP 800-53 Rev 4]

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. [FIPS 200]

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). [NIST SP 800-53 Rev 4]

Mission Critical Information - Information that if lost, misused, disclosed, accessed without authorization, or modified without authorization, would have a debilitating impact on the mission of the College. [NIST SP 800-60 Vol 1 Rev 1, adapted]

Mobile Device - A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. [NIST SP 800-53 Rev 4]

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. [NIST SP 800-53 Rev 4]

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. [CNSSI 4009]

Nonlocal Maintenance - Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. [NIST SP 800-53 Rev 4]

Non-Organizational User - A user who is not an organizational user (including public users). [NIST SP 800-53 Rev 4]

Organizational User - An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship. [NIST SP 800-53 Rev 4]

Personal Identifying Information (PII) - Information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Penal Code. [BCC Sec 521.002(a)(1)]

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. [OMB Memorandum 02-01]

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). [NIST SP 800-53 Rev 4]

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. [FIPS 199, adapted]

Procedure - Instructions to assist information security staff, custodians, and users in implementing policies, standards, and guidelines. [1 Tex. Admin. Code §202.1(29)]

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 organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). [NIST SP 800-53 Rev 4]

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). [CNSSI 4009]

Residual Risk - The risk that remains after security controls have been applied. [1 Tex. Admin. Code §202.1(30)]

Risk - The effect on the entity's missions, functions, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact. Risk outcomes are a consequence of Impact levels defined in this section. [1 Tex. Admin. Code §202.1(31)]

Risk Assessment - The process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls. [1 Tex. Admin. Code §202.1(32)]

Risk Management - The process of aligning information resources risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures. [1 Tex. Admin. Code §202.1(33)]

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [CNSSI 4009]

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. [NIST SP 800-53 Rev 4]

Security Assessment - See Security Control Assessment.

Security Assessment Plan - The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. [NIST SP 800-53 Rev 4]

Security Categorization - The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See Security Category. [NIST SP 800-53 Rev 4]

Security Category - The characterization of information or an information system 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 organizational operations, organizational assets, individuals, and other organizations. [NIST SP 800-53 Rev 4, adapted]

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. [NIST SP 800-53 Rev 4]

Security Control Assessment - The testing or evaluation of security controls 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 an information system or organization [NIST SP 800-53 Rev 4]

Security Incident - An event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources. [1 Tex. Admin. Code §202.1(34)]

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. [NIST SP 800-53 Rev 4]

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. [1 Tex. Admin. Code §213.1(14)]

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 - (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual. [BCC Sec. 521.002(a)(2)]

Server - A physical or virtual computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). [NIST SP 800-47, adapted]

Site Policies Page - A web page containing website policies or a link to each policy. [1 Tex. Admin. Code §206.1(19)]

Software - Computer programs and associated data that may be dynamically written or modified during execution. [CNSSI 4009]

Standards - Specific mandatory controls that help enforce and support the information security policy. [1 Tex. Admin. Code §202.1(26)]

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. [CNSSI 4009]

System Security Plan - 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. [NIST SP 800-18]

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST SP 800-53 Rev 4]

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals. [BCC Sec 521.002(a)(2)]

TRAIL - Texas Records and Information Locator, or its successor, providing a method to do a statewide search. [1 Tex. Admin. Code §206.1(21)]

Transaction Risk Assessment - An evaluation of the security and privacy required for an interactive web session providing public access to government information and services. [1 Tex. Admin. Code §206.1(22)]

Unauthorized Disclosure - An event involving the exposure of information to entities not authorized access to the information. [NIST SP 800-57 Part 3]

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. [NISTIR 7621 Rev 1]

User - An individual, process, or automated application authorized to access an information resource in accordance with federal and state law, agency policy, and the information-owner's procedures and rules. [1 Tex. Admin. Code §202.1(38)]

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. [1 Tex. Admin. Code §213.1(19)]

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSSI 4009]

Vulnerability Assessment - A documented evaluation containing information described in §2054.077(b), Texas Government Code which includes the susceptibility of a particular system to a specific attack. [1 Tex. Admin. Code §202.1(39)]

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. [1 Tex. Admin. Code §206.1(24)]

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. [NISTIR 7693]

Wireless Network - A network using wireless technology that permits the transfer of information between separated points without physical connection. [CNSSI 4009, adapted]

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

A

Accessibility testing....16
Acronyms....4

C

Censorship....8
Chapter VIII of TSUS Regents' Rules....19
Children's Online Privacy Protection Act of 1998....21
Computer Software Rental Amendments Act of 1990....12
Copyright Law....8, 11

D

Digital Millennium Copyright Act....11
Director of Public Information....19

E

EIR Accessibility Coordinator....15
Electronic Communications Privacy Act....12

F

Federal Information Security Management Act of 2002 (FISMA)....12

G

Glossary....4

H

Health Insurance Portability and Accountability Act (HIPAA)....12

I

Information Resources Manager (IRM)....4
Information Security Officer (ISO)....4, 5, 23, 30
Intellectual Property....8

L

Lamar State College Port Arthur Brand Guide....20, 21

P

Passwords....9, 11, 41

S

Section 39.02(a) of the Texas Penal Code....19

T

Texas Administrative Code
1 Tex. Admin. Code § 202.70....6
1 Tex. Admin. Code § 202.71....6
1 Tex. Admin. Code §202....22
1 Tex. Admin. Code §202.70....29
1 Tex. Admin. Code §202.70-76....11, 12
1 Tex. Admin. Code §202.71....29
1 Tex. Admin. Code §202.72....29
1 Tex. Admin. Code §202.73....29
1 Tex. Admin. Code §202.74....29
1 Tex. Admin. Code §202.75....29
1 Tex. Admin. Code §206....21
1 Tex. Admin. Code §206.70....17
1 Tex. Admin. Code §206.72....21
1 Tex. Admin. Code §206.73....20
1 Tex. Admin. Code §206.74....20
1 Tex. Admin. Code §206.74(b)....20
1 Tex. Admin. Code §206.74(c)....21
1 Tex. Admin. Code §206.74(d)....21
1 Tex. Admin. Code §213....18, 21
1 Tex. Admin. Code §213.35....17
1 Tex. Admin. Code §213.36....17
Texas Government Code §2054 Subchapter D....6
Texas Government Code §2054.071....4
Texas Government Code §2054.074....4
Texas Government Code §2054.133....23, 28, 29
Texas Government Code §2054.457....18
Texas Government Code §2054.460....14, 18
Texas Government Code §556.004....12
Texas Penal Code
Texas Penal Code, §37.10: Tampering with Governmental Record....11, 12
Texas Penal Code, Chapter 33: Computer Crimes..11, 12

The Federal Family Educational Rights and Privacy Act....11
TSUS Sexual Misconduct Policy and Procedures.....12

U

United States Code, Title 18, Chapter 47, §1030: Fraud and Related Activity in Connection with Computers.....11, 12

V

Voluntary Product Accessibility Template (VPAT)..... 15

W

Website 19
Content Owner 20
Personal Identifying Information (PII)..... 21