



LAMAR STATE COLLEGE - PORT ARTHUR

COMPUTER SERVICES DEPARTMENT

INFORMATION RESOURCES POLICIES

(Revised November 2007)

**INFORMATION RESOURCES POLICIES
TABLE OF CONTENTS**

| | | |
|-------------|--|-----------|
| I. | Overview | 3 |
| | <i>A. Introduction</i> | <i>3</i> |
| | <i>B. Purpose and Scope</i> | <i>3</i> |
| | <i>C. References</i> | <i>3</i> |
| II. | Roles and Responsibilities | 4 |
| | <i>A. Generic Roles</i> | <i>4</i> |
| | <i>B. Specific Responsibilities</i> | <i>5</i> |
| III. | Security Violations and Sanctions | 9 |
| | <i>A. Detecting and Reporting</i> | <i>9</i> |
| | <i>B. Sanctions</i> | <i>9</i> |
| | <i>C. Disciplinary Actions</i> | <i>9</i> |
| IV. | Disaster Recovery/Business Contingency Plan | 10 |
| V. | Information Resources Policies | 11 |
| | <i>A. Information Resources Security Policies</i> | <i>11</i> |
| | <i>Physical Access (5.16.1)</i> | <i>11</i> |
| | <i>Change Management (5.16.2)</i> | <i>13</i> |
| | <i>Information Systems Privacy (5.16.3)</i> | <i>15</i> |
| | <i>Security Training (5.16.4)</i> | <i>18</i> |
| | <i>Security Monitoring (5.16.5)</i> | <i>19</i> |
| | <i>Intrusion Detection (5.16.6)</i> | <i>21</i> |
| | <i>Incident Management (5.16.7)</i> | <i>23</i> |
| | <i>Network Access (5.16.8)</i> | <i>25</i> |
| | <i>Network Configuration (5.16.9)</i> | <i>27</i> |
| | <i>Server Hardening (5.16.10)</i> | <i>29</i> |
| | <i>Account Management (5.16.11)</i> | <i>31</i> |
| | <i>Administrator/Special Access (5.16.12)</i> | <i>34</i> |
| | <i>Password Security (5.16.13)</i> | <i>36</i> |
| | <i>Portable Computing (5.16.14)</i> | <i>39</i> |
| | <i>Vendor Access (5.16.15)</i> | <i>40</i> |
| | <i>Backup (5.16.16)</i> | <i>42</i> |
| | <i>Virus Protection (5.16.17)</i> | <i>44</i> |
| | <i>System Development (5.16.18)</i> | <i>45</i> |
| | <i>B. Information Resources Use Policies</i> | <i>46</i> |
| | <i>Acceptable Use (5.16.19)</i> | <i>46</i> |
| | <i>Internet (5.16.20)</i> | <i>49</i> |
| | <i>E-Mail (5.16.21)</i> | <i>52</i> |
| | <i>Instant Messaging (5.16.22)</i> | <i>54</i> |
| | <i>Peer-to-Peer (P2P) (5.16.23)</i> | <i>56</i> |
| | <i>Software Licensing (5.16.24)</i> | <i>58</i> |
| | <i>Computing Facilities Use (5.16.25)</i> | <i>61</i> |
| | <i>Telephone Systems (5.16.26)</i> | <i>63</i> |
| VI. | Appendices | |
| | <i>Appendix A: Administrative Systems Assets/Custodians</i> | <i>64</i> |
| | <i>Appendix B: Information Resources Policies Maintenance</i> | <i>65</i> |
| | <i>Appendix C: Definitions</i> | <i>66</i> |
| | <i>Appendix D: Standard Policy Statements</i> | <i>72</i> |
| | <i>Appendix E: Software/Hardware Selection, Budgeting, and Acquisition</i> | <i>74</i> |

POLICY: INFORMATION RESOURCES
SCOPE: FACULTY, STAFF, AND STUDENTS
POLICY NUMBER: 5.16
REVISED: SEPTEMBER 2007

I. Overview

A. *Introduction*

Lamar State College - Port Arthur relies heavily on computers and the automated retrieval, processing, and storage of information to meet its operational, financial, and reporting requirements. Continuing availability of information is essential to the operation of College functions. Moreover, increased use of automation and technical advances in automation processing will increase continual dependence on information resources. Information processed by computers is a critical asset and must be protected accordingly. Information use and security requires the active support and ongoing participation of executive, technical, and non-technical management, as well as all students, faculty, administrative and technical personnel whose duties or activities bring them in contact with critical, confidential, or sensitive information resources.

B. *Purpose and Scope*

In 1993, the Texas Department of Information Resources (DIR) published Information Use and Security Standards which have been adopted in the Texas Administrative Code establishing state policy regarding information security. The purpose of this manual is to document the Information Security Program instituted at the College to comply with state security policy and standards and hence, protect these valuable assets against accidental or unauthorized disclosure, modification, or destruction, as well as to assure the security, reliability, integrity, and availability of information. Protecting information and the investment that surrounds it is the impetus for establishing an information security program. Information security applies to mainframe, minicomputer, microcomputer, distributed processing, and networking environments. It applies to administrative as well as academic computing.

C. *References*

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

II. Roles and Responsibilities

Information resources proper use, security, and risk management requires the active support and ongoing participation of individuals from all levels. It requires the support of executive, technical, and non-technical management, as well as all students, faculty, administrative and technical personnel whose duties or activities bring them in contact with critical, confidential, or sensitive information resources.

A. *Generic Roles*

The College recognizes four generic roles that individuals and entities possess with respect to the proper use and security of information resources. Circumstances will determine which role (or roles) is attributable to a particular individual or entity in any given situation. The roles are owner, custodian, agent, and user.

1. **Owner**

The Owner of information resources described in this manual is Lamar State College - Port Arthur, for and on behalf of the State of Texas. The College's responsibility as owner stems mainly from its charge to be a good steward of the assets entrusted to its care, and to use them wisely in the pursuit of its mission.

2. **Custodian**

The Custodian of information resources is the individual upon whom responsibility rests for carrying out the function that is supported by or uses the resources. At the College, the role of custodian is normally performed by managers, supervisors, and security administrators (see descriptions in the section on specific responsibilities below). Generally speaking, custodians are responsible for:

- a. Reviewing requests for access to the information resource and approving or denying such requests.
- b. Implementing service agreements with agents for development, acquisition, and/or support of the resource.
- c. Judging the value of the resource with respect to criticality, confidentiality, and sensitivity.
- d. Specifying access control requirements and conveying them to users and agents.

3. **Agent**

An Agent is the entity that provides technical facilities, software development, data processing, telecommunications, printing, and other support services to custodians and users of automated information. Agent responsibility resides with any person or group charged with the physical possession or control of information assets by custodians and College management. The Computer Service Department is the predominant agent (see descriptions in the section on specific responsibilities below), but the College's contractors and third party vendors may also perform this role. Generally speaking, agents are responsible for:

- a. Implementing the controls specified by the custodian.
- b. Providing physical and procedural safeguards for the information resources in their possession, under their control, and/or within facilities managed by the agent.
- c. Assisting custodians in evaluating the effectiveness of controls.
- d. Facilitating access to the information resources and making cost effective provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources.

4. User

Users of an information resource are individuals or automated applications that are authorized access to the resource by the custodian, in accordance with the custodian's procedures and rules. Generally, users are responsible for:

- a. Using a resource only for the purposes specified by its custodian.
- b. Complying with controls established by the custodian.
- c. Complying with applicable federal, state, and College security laws, policies and procedures.
- d. Preventing disclosure of sensitive information.
- e. Identifying security vulnerabilities and inform management and the Information Security Function of those vulnerabilities.
- f. Reporting any known or observed attempted security violations.

B. Specific Responsibilities

1. College President

It is the President's role to assure that the College's information assets are used properly and protected from the effects of damage, destruction, accidental or unauthorized disclosure, contamination, or modification, as well as to ensure the security, reliability, integrity, and availability of information. The President is responsible for establishing and maintaining an information security and risk management program within the College. The President retains ultimate responsibility for enforcement of all security and risk management policies but may delegate the remaining responsibilities to the Director of Computer Services or a designee.

2. Information Resources Manager (IRM)

The IRM is the person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3. Computer Services Personnel

Generally speaking, Computer Services personnel operate in the role of agents for other members of the College community. The department provides the computing infrastructure necessary to obtain, implement, house, operate and secure information resources. Because of the nature of their work and their proximity to all types of computer resident and non-computer resident data, personnel in Computer Operations are particularly vulnerable to the inadvertent disclosure of confidential or sensitive information.

Computer Services personnel will treat all user data as confidential. Data will not be released or discussed with other personnel without the express prior consent of the user or designated custodian of that data. Situations may arise when it appears necessary to make an exception to this rule. Such exceptions may be made only with the approval of the Director of Computer Services and must be reported within a reasonable time to the designated custodian of the affected data.

Any request for data accessible via the College computer network is always referred to the custodian of the information and is never handled directly by the Computer Services staff. For example, requests for transcript or GPA information should be directed to the Registrar's

Office (the designated custodian of official transcript information).

The Director of Computer Services is also the Information Security Officer (ISO) at the College. Other Computer Services personnel function as Security Operators. The ISO and other designated staff have the responsibilities listed below for centrally administered systems, LANs, labs, and applications. The focus and level (primary, secondary, etc.) of each Information Security Function (ISF) responsibility will be different for each member of the ISF staff, depending on the specific information resource involved.

- a. Develop, implement, and maintain the college's information security and risk management program including a risk analysis process.
- b. Identify vulnerabilities that may cause inappropriate or accidental access, destruction, or disclosure of information, and establish security controls necessary to eliminate or minimize their potential effects.
- c. Ensure the college's critical and sensitive information resources are identified, that all information resources are assigned to a custodian, and that the duties of custodians are prescribed.
- d. Ensure that managers and users are provided necessary technical support services with which to define and select cost effective security controls, policies, and procedures.
- e. Develop and maintain a contingency plan for information resources services resumption to protect the College against the potential effects of a disaster, in cooperation with College management and the custodians and users of information.
- f. Keep management aware of legal and regulatory changes affecting information privacy and computer crime.
- g. Provide College-wide security consulting services and serves as the College's internal and external point of contact on information security matters.
- h. Manage the development, implementation, and testing of security controls and methods for their evaluation.
- i. Report to management periodically on College security posture and progress, including problem areas with recommended enhancements.
- j. Implement cost effective security controls as necessary to identify actual or attempted violations of security policies.
- k. Establish procedures necessary to monitor and ensure compliance with established security and risk management policies and procedures.
- l. Coordinate with College managers on matters related to the planning, development, implementation, or modification of information security and risk management policies and procedures that will affect the College.
- m. Establish adequate information security awareness programs to assure that College staff (with particular emphasis on the custodians, agents and users of information) are educated and aware of their roles and responsibilities relative to information security and risk management.

4. Other College Personnel

a. Managers

Managers (administrative heads, account managers, etc.) operate as custodians to assure protection of the information resources utilized in carrying out programs under their direction. Specifically, managers have the following custodianship responsibilities in relation to the College information security and risk management program:

- (1) Participate in the College's risk analysis process by identifying assets and assessing their value to their functional unit and to the College.
- (2) Ensure proper classification of the automated information resources in their custody with respect to criticality, confidentiality, and sensitivity.

- (3) Work with agents, security administrators, technical staff and the ISF in identifying and selecting appropriate and cost-effective security controls and procedures to protect the information assets in their custody.
- (4) Define the appropriate security requirements for user access to automated information files and databases for which the function has custodianship responsibility.
- (5) Ensure that the access privileges of individuals are granted, revoked, and periodically reviewed as necessary to assure the utility and security of the information assets in their custody.
- (6) Define and develop quality assurance procedures to minimize the risk of errors and omissions and to ensure the integrity of data for which the function has custodianship responsibility.

b. Security Administrator

The Security Administrator operates primarily as the custodian of information resources; this function is performed by the Director of Computer Services who reports to the Vice President for Academic Affairs. The Administrator is responsible for identifying and applying the available access controls as appropriate to ensure that only authorized individuals or groups have access to the information resources in their custody.

Specifically, the Security Administrator has the following custodian and agent responsibilities in relation to the College information security and risk management program:

- (1) Participate in the College's risk analysis process by identifying threats to information assets and assessing the risk associated with those threats.
- (2) Assist managers in properly classifying automated information resources with respect to criticality, confidentiality, and sensitivity.
- (3) Work with agents, managers, technical staff, internal audit, and the ISF in identifying and selecting appropriate and cost-effective security controls and procedures to protect the information assets in their custody.
- (4) Assist managers and agents in implementing the appropriate security requirements for user access to automated information files and databases for which the function has custodianship responsibility.
- (5) Grant, revoke, and periodically review the access privileges of individuals as necessary to assure the utility and security of the information assets in their custody.
- (6) Ensure that valid user lists are current and auditable.
- (7) Oversee procedures for College password control.

c. Other Personnel

All personnel have a responsibility for maintaining the security and confidentiality of the College's information assets and each individual must comply with the College's information security policies and procedures. These policies and procedures are described further in Section IV of this manual.

5. Internal Audit Personnel

Internal Auditors operate in an oversight role by reviewing the adequacy of the College's information resources policies, procedures, and controls. Specifically, Internal Auditors have the following responsibilities in relation to the College's security and risk management efforts.

The internal audit function is performed by internal audit staff housed at Lamar University and report to the Texas State University System (TSUS). Duties include:

- a. Examine the College's information security policies and procedures for compliance with state information security and risk management policies and standards.
- b. Examine the effectiveness of the College's information security policies and procedures, identify inadequacies within the existing security and risk management program, identify possible corrective actions, and inform management, the ISF, custodians, agents, and users of its findings.
- c. Review and evaluate the effectiveness of controls for automated information systems that are either under development or operational, with particular emphasis on major systems.
- d. Participate in the College risk analysis process.

III. Security Violations and Sanctions

Information resources are valuable assets strategically provided to further research, education, public service, and administrative functions of the College. Individuals using information resources owned or managed by the College are expected to know and comply with College policies, procedures, and local, state and federal laws. Individuals are responsible for the security of any computer account issued to them and will be held accountable for any activity that takes place in their account.

In September 1985, the Texas Computer Crimes Statute became operative as part of the Texas Penal Code. Under this state law, it is a crime to make unauthorized use of protected computer systems or data files on computers, or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges from Class B misdemeanor to third-degree felony.

A. *Detecting and Reporting*

Users of College information resources are expected to report any known or observed attempted security violation. Additionally, they must not conceal or help to conceal violations by any party. For centrally administered computing facilities or other sites accessible via the Internet, any actual or suspected security violation should be reported immediately to the Director of Computer Services at 409-984-6484 or to the Assistant Director of Systems, Networking, and Telecom at 409-984-6141.

For computing facilities administered by other departments, any actual or suspected security violation should be reported to the appropriate Dean, Director, or Department Head and to the Director of Computer Services.

Within Computer Services, the administrative system monitors and generates logs and warnings on system activity. These documents are reviewed daily and, in the case, of possible illegal access attempts, at the time of occurrence by departmental staff. System custodians are required to review reports on administrative system users and their access on a semi-annual basis.

B. *Sanctions*

Users of College computing resources are prohibited from making attempts to violate the security of other computer users on any system accessible via the College computer network. The violation or attempted violation of network or system security is grounds for revocation of computer access privileges, suspension, or discharge of employees, suspension or expulsion of students, and possible prosecution to the fullest extent of the law.

C. *Disciplinary Actions*

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries, a termination of employment relations in the case of contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Lamar State College - Port Arthur Information Resources access privileges, civil, and criminal prosecution, as well as legal action under state and federal laws, and legal action by the owners and licensors of proprietary software for violation of copyright laws and license agreements.

IV. Disaster Recovery/Business Continuity Plan

The Computer Services Department is responsible for developing and maintaining a Disaster Preparedness/Recovery/Business Continuity Plan designed to address the operational restoration of the college's critical computer processing capability. This plan identifies the strategy to recover centrally administered data storage, programs, and processing capability in the event of a disaster. The plan includes an inventory of critical hardware and software information resources. It also identifies the minimum acceptable recovery configuration, which must be available for the College to resume the minimum required levels of essential services. The plan is located in strategic areas and available to all Computer Services personnel through a shared network resource. The plan contains personal and proprietary information and thus will not be published on the Web.

The Computer Services Disaster Preparedness/Recovery Plan described above does not address the needs of individual operating units beyond the restoration of access to their critical centrally administered applications. The Computer Services Disaster Preparedness/Recovery Plan is a component of the Lamar State College – Port Arthur Disaster Preparedness/Recovery/Business Continuity Plan. All major College divisions/departments have developed individual plans for protecting their information resource assets and operating capability. Each departmental plan addresses losses ranging from minor temporary outages to catastrophic.

The Lamar State College – Port Arthur Disaster Preparedness/Recovery/Business Continuity Plan is located in the offices of the president, vice presidents, and other strategic locations around the campus.

V. Information Resources Policies

A. Information Resources Security Policies

5.16.1 Physical Security Policy

5.16.1.1 Introduction

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program.

5.16.1.2 Purpose

The purpose of the Lamar State College - Port Arthur Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

5.16.1.3 Audience

The Lamar State College - Port Arthur Physical Access Policy applies to all individuals within the Lamar State College - Port Arthur enterprise who are responsible for the installation and support of Information Resource, individuals charged with Information Resources Security, and data owners.

5.16.1.4 Policy

- All physical security systems must comply with applicable all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Resources restricted facilities must be documented and managed.
- All IR facilities must be physically protected in proportion to the criticality or importance of their function at Lamar State College - Port Arthur.
- Access to Information Resources facilities must be granted only to Lamar State College - Port Arthur support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.
- Each individual who is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Requests for access must come from the applicable Lamar State College - Port Arthur data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.

- Cards and/or keys must not have identifying information other than a return mail address.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals who change roles within Lamar State College - Port Arthur or are separated from their relationship with Lamar State College - Port Arthur
- Visitors must be escorted in card access controlled areas of Information Resources facilities.
- The person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals who no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

5.16.1.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 2, 3, 4, 5, 8, 9, 16, and 19 in appendix D.

5.16.2 Change Management Policy

5.16.2.1 Introduction

The Information Resources infrastructure at Lamar State College - Port Arthur is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

5.16.2.2 Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community, and to increase the value of Information Resources.

5.16.2.3 Audience

The Lamar State College - Port Arthur Change Management Policy applies to all individuals who install, operate or maintain Information Resources.

5.16.2.4 Policy

- Every change to a Lamar State College - Port Arthur Information Resources resource, such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy, and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to, or coordinated with the leader of the change management process.
- A Change Management Committee, appointed by Computer Services Leadership, will meet regularly to review change requests, and to ensure that change reviews and communications are being satisfactorily performed.
- A formal written change request must be submitted for all changes, both scheduled and unscheduled.
- All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change.
- The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key

business process, such as year end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

- Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
 - ❖ Date of submission and date of change
 - ❖ Owner and custodian contact information
 - ❖ Nature of the change
 - ❖ Indication of success or failure
- All Lamar State College - Port Arthur information systems must comply with an Information Resources change management process that meets the standards outlined above.

5.16.2.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 12, 14, and 15 in appendix D.

5.16.3 Information Systems Privacy Policy

5.16.3.1 Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of Lamar State College - Port Arthur Information Resources. Internal users should have no expectation of privacy with respect to Information Resources. External users should have the expectation of complete privacy, except in the case of suspected wrongdoing, with respect to Information Resources.

5.16.3.2 Purpose

The purpose of the Lamar State College - Port Arthur Computer Services Privacy Policy is to clearly communicate the Lamar State College - Port Arthur Computer Services Privacy expectations to Information Resources users.

5.16.3.3 Audience

The Lamar State College - Port Arthur Computer Services Privacy Policy applies equally to all individuals who use any Lamar State College - Port Arthur Information Resource.

5.16.3.4 Ownership

Electronic files created, sent, received, or stored on computers owned, leased administered, or otherwise under the custody and control of Lamar State College - Port Arthur are the property of Lamar State College - Port Arthur.

5.16.3.5 Policy

- Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of Lamar State College - Port Arthur are not private and may be accessed by Lamar State College - Port Arthur Computer Services employees at any time without knowledge of the IR user or owner.
- To manage systems and enforce security, Lamar State College - Port Arthur may log, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, Lamar State College - Port Arthur may also capture User activity such as telephone numbers dialed and web sites visited.
- A wide variety of third parties have entrusted their information to Lamar State College - Port Arthur for business purposes, and all workers at Lamar State College - Port Arthur must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual student; student personal information is accordingly confidential and access will be strictly limited based on business need for access.
- Users must report any weaknesses in Lamar State College - Port Arthur computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on Lamar State College - Port Arthur systems for which they do not have authorization or explicit consent.

5.16.3.6 Public Access Privacy Policy

Lamar State College - Port Arthur web sites available to the general public must contain a Privacy Statement. An example of a good public Privacy Statement follows:

Web site Privacy Statement on the Use of Information Gathered from the General Public

The following statement applies only to members of the general public and is intended to address concerns about the types of information gathered from the public, if any, and how that information is used:

I. Cookies

A “cookie” is a small file containing information that is placed on a user’s computer by a web server. Typically, these files are used to enhance the user’s experience of the site, to help users move between pages in a database, or to customize information for a user.

Any information that Lamar State College - Port Arthur 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 Lamar State College - Port Arthur is legally required to do so in connection with law enforcement investigations or other legal proceedings.

II. Logs and Network Monitoring

Lamar State College - Port Arthur 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:

Hostname: the hostname and/or 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., Netscape 4 for Windows, IE 4 for Macintosh, etc.)

Referrer: 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 and 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 1.0, ftp, etc.

The above information is not used in any way that would reveal personally identifying information to outside parties unless Lamar State College - Port Arthur is legally required to do so in connection with law enforcement investigations or other legal proceedings.

III. Email and Form Information

If a member of the general public sends Lamar State College - Port Arthur an e-mail 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 government agency or person who 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 System Administration is legally required to do so in connection with law enforcement investigations or other legal proceedings.

IV. Links

This site may contain links to other sites. Lamar State College - Port Arthur is not responsible for the privacy practices or the content of such websites.

V. Security

This site has security measures in place to protect from loss, misuse and alteration of the information.

Contacting Lamar State College - Port Arthur

If there are any questions about this privacy statement, the practices of this site, or dealings with this website, contact

Samir.Ghorayeb@lamarpa.edu

5.16.3.7 Supporting Information

This Policy is supported by the following Security Policy Standards references 2, 3, and 16 in appendix D.

5.16.4 Security Training Policy

5.16.4.1 Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific, and training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

5.16.4.2 Purpose

The purpose of the Security Training Policy is to describe the requirements for ensure each user of Lamar State College - Port Arthur Information Resources is receives adequate training on computer security issues.

5.16.4.3 Audience

The Lamar State College - Port Arthur Security Training Policy applies equally to all individuals who use any Lamar State College - Port Arthur Information Resources.

5.16.4.4 Policy

- All new users must attend an approved Security Awareness training class prior to, or at least within 30 days of, being granted access to any Lamar State College - Port Arthur information resources.
- All users must sign an acknowledgement stating they have read and understand Lamar State College - Port Arthur requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect Lamar State College - Port Arthur information resources.
- Computer Services must prepare, maintain, and distribute one or more information security manuals that concisely describe Lamar State College - Port Arthur information security policies and procedures.
- All users must attend an annual computer security compliance seminar and pass the associated examination.
- Computer Services must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

5.16.4.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 2 and 3 in appendix D.

5.16.5 Security Monitoring Policy

5.16.5.1 Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files.

5.16.5.2 Purpose

The purpose of the Security Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

5.16.5.3 Audience

The Lamar State College - Port Arthur Security Monitoring Policy applies to all individuals who are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

5.16.5.4 Policy

- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
 - ❖ Internet traffic
 - ❖ Electronic mail traffic
 - ❖ LAN traffic, protocols, and device inventory
 - ❖ Operating system security parameters
- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
 - ❖ Automated intrusion detection system logs
 - ❖ Firewall logs
 - ❖ User account logs
 - ❖ Network scanning logs
 - ❖ System error logs
 - ❖ Application logs
 - ❖ Data backup and recovery logs
 - ❖ Help desk trouble tickets
 - ❖ Telephone activity – Call Detail Reports

- ❖ Network printer and fax logs
- The following checks will be performed at least annually by assigned individuals:
 - ❖ Password strength
 - ❖ Unauthorized network devices
 - ❖ Unauthorized personal web servers
 - ❖ Unsecured sharing of devices
 - ❖ Unauthorized modem use
 - ❖ Operating System and Software Licenses
- Any security issues discovered will be reported to the ISO for follow-up investigation.

5.16.5.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 5, 6, 16, and 17 in appendix D.

5.16.6 Intrusion Detection Policy

5.15.6.1 Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

5.16.6.2 Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

5.16.6.3 Audience

The Lamar State College - Port Arthur Intrusion Detection Policy applies to all individuals who are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resources Security.

5.16.6.4 Intrusion Detection Policy

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control system must be enabled.
- Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.
- System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
- Audit logs for servers and hosts on the internal, protected, network must be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the ISO.
- Host based intrusion tools will be checked on a routine.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Policy.
- Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the Computer Services Help Desk.

5.15.6.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 14, 16, and 17 in appendix D.

5.16.7 Incident Management Policy

5.16.7.1 Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

5.16.7.2 Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy.

5.16.7.3 Audience

The Lamar State College - Port Arthur Incident Management Policy applies equally to all individuals who use any Lamar State College - Port Arthur Information Resources.

5.16.7.4 Incident Management Practice Standard

- Lamar State College - Port Arthur CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The ISO, working with the IRM, will determine if a widespread Lamar State College - Port Arthur communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
- The Lamar State College - Port Arthur ISO is responsible for reporting the incident to the:
 - ❖ IRM

- ❖ Department of Information Resources as outlined in TAC 202
- ❖ Local, state or federal law officials as required by applicable statutes and/or regulations
- The ISO is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.
- In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and Lamar State College - Port Arthur.

5.16.7.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 3, 6, 7, 16, 21, and 22 in appendix D.

5.16.8 Network Access Policy

5.16.8.1 Introduction

The Lamar State College - Port Arthur network infrastructure is provided as a central utility for all users of Lamar State College - Port Arthur Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet Lamar State College - Port Arthur demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

5.16.8.2 Purpose

The purpose of the Lamar State College - Port Arthur Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of Lamar State College - Port Arthur information.

5.16.8.3 Audience

The Lamar State College - Port Arthur Network Access Policy apply equally to all individuals with access to any Lamar State College - Port Arthur Information Resource.

5.16.8.4 Policy

- Users are permitted to use only those network addresses issued to them by Lamar State College - Port Arthur IS.
- All remote access (dial in services) to Lamar State College - Port Arthur will be either through an approved modem pool or via an Internet Service Provider (ISP).
- Remote users may connect to Lamar State College - Port Arthur Information Resources only through an ISP and using protocols approved by Lamar State College - Port Arthur.
- Users inside the Lamar State College - Port Arthur firewall may not be connected to the Lamar State College - Port Arthur network at the same time a modem is being used to connect to an external network.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Lamar State College - Port Arthur network without Lamar State College - Port Arthur Computer Services approval.
- Users must not install network hardware or software that provides network services without Lamar State College - Port Arthur Computer Services approval.
- Non Lamar State College - Port Arthur computer systems that require network connectivity must conform to Lamar State College - Port Arthur Computer Services Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, Lamar State College - Port Arthur users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Lamar State College - Port Arthur network infrastructure.
- Users are not permitted to alter network hardware in any way.

5.16.8.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 5, 6, and 20 in appendix D.

5.16.9 Network Configuration Policy

5.16.9.1 Introduction

The Lamar State College - Port Arthur network infrastructure is provided as a central utility for all users of Lamar State College - Port Arthur Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

5.16.9.2 Purpose

The purpose of the Lamar State College - Port Arthur Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of Lamar State College - Port Arthur information.

5.16.9.3 Audience

The Lamar State College - Port Arthur Network Configuration Policy applies equally to all individuals with access to any Lamar State College - Port Arthur Information Resource.

5.16.9.4 Policy

- Lamar State College - Port Arthur Computer Services owns and is responsible for the Lamar State College - Port Arthur network infrastructure and will continue to manage further developments and enhancements to this infrastructure
- To provide a consistent Lamar State College - Port Arthur network infrastructure capable of exploiting new networking developments, all cabling must be installed by Lamar State College - Port Arthur Computer Services or an approved contractor.
- All network connected equipment must be configured to a specification approved by Lamar State College - Port Arthur Computer Services.
- All hardware connected to the Lamar State College - Port Arthur network is subject to Lamar State College - Port Arthur Computer Services management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of Lamar State College - Port Arthur Computer Services.
- The Lamar State College - Port Arthur network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by Lamar State College - Port Arthur Computer Services.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by Lamar State College - Port Arthur Computer Services.
- All connections of the network infrastructure to external third party networks is the responsibility of Lamar State College - Port Arthur Computer Services. This includes connections to external telephone networks.
- Lamar State College - Port Arthur Computer Services Firewalls must be installed and configured following the Lamar State College - Port Arthur Firewall Implementation Standard documentation.
- The use of departmental firewalls is not permitted without the written authorization from Lamar State College - Port Arthur Computer Services.

- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Lamar State College - Port Arthur network without Lamar State College - Port Arthur Computer Services approval.
- Users must not install network hardware or software that provides network services without Lamar State College - Port Arthur Computer Services approval.
- Users are not permitted to alter network hardware in any way.

5.16.9.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 12, 15, 19, and 20 in appendix D.

5.16.10 Server Hardening Policy

5.16.10.1 Introduction

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service

5.16.10.2 Purpose

The purpose of the Lamar State College - Port Arthur Server Hardening Policy document is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

5.16.10.3 Audience

The Lamar State College - Port Arthur Server Hardening Policy applies to all individuals who are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

5.16.10.4 Policy

- A server must not be connected to the Lamar State College - Port Arthur network until it is in a Lamar State College - Port Arthur Computer Services Department accredited secure state and the network connection is approved by Lamar State College - Port Arthur Computer Services Department.
- The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for Lamar State College - Port Arthur Computer Services Department accreditation. Some of the general steps included in the Server Hardening Procedure include:
 - ❖ Installing the operating system from an Computer Service Department approved Source
 - ❖ Applying vendor supplied patches
 - ❖ Removing unnecessary software, system services, and drivers
 - ❖ Setting security parameters, file protections and enabling audit logging
 - ❖ Disabling or changing the password of default accounts
- Lamar State College - Port Arthur Computer Services Department will monitor security issues, both internal to Lamar State College - Port Arthur and externally, and will manage the release of security patches on behalf of Lamar State College - Port Arthur.
- Lamar State College - Port Arthur Computer Services Department will test security patches against Computer Services Department core resources before release where practical.
- Lamar State College - Port Arthur Computer Services Department may make hardware resources available for testing security patches in the case of special applications.
- Security patches must be implemented within the specified timeframe of notification from Lamar State College - Port Arthur Computer Services Department.

5.16.10.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 8, 11, 16, and

17 in appendix D.

5.16.11 Account Management Policy

5.16.11.1 Introduction

Computer accounts are the means used to grant access to Lamar State College - Port Arthur Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

5.16.11.2 Purpose

The purpose of the Lamar State College - Port Arthur Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

5.16.11.3 Audience

The Lamar State College - Port Arthur Account Management Security Policy applies equally to all individuals with authorized access to any Lamar State College - Port Arthur Information Resources.

5.16.11.4 Policy

- All Lamar State College – Port Arthur information resources users will be granted access through a computer account in the following manner:
 - Email Accounts:
 - Students: An Email Account will automatically be created upon satisfactory admission to the college. Admission status is defined by the Office of Admission and Records. Student Email Accounts will remain active permanently but are subject to the account and password expiration and security policies.
 - Employees: An Email Account will automatically be created upon active employment with the college. Employment status is defined by the Human Resources Office. Employee/Non-Student Email Accounts will be disabled upon the employee separation from the college and a written request from the Human Resources Office. An employee may submit a written request to the Director of Computer Service to extend the life of that account for a period that shall not exceed 90 days. All account will be reviewed semi-annually and stale accounts will be deleted accordingly.
 - Special Users: An Email Account will be created only at the request of a department head. Approved by the Vice President of that department and the Director of Computer Services is required. Examples of special users are Auditors and Vendors. This type of account must have an expected expiration date. Special Email Accounts will be deleted when expired unless a written request is submitted by the department head justifying the need to extend the life of the account to the Director of Computer Services.
 - Network Accounts:
 - This type of account is intended for the purpose of accessing local Information Resources (printers, network shares, disk space, internet, etc...). These accounts are monitored very closely as they provide access to many critical information resource.
 - Students: Accounts will automatically be created upon satisfactory admission to the college. Admission status is defined by the Office of Admission and

Records. Student Network Accounts will remain active as long as the student is currently enrolled and using that account. These accounts will be disabled immediately if the student either withdraws from the college or lack of use for a period of 120 days. All account will be reviewed semi-annually and stale accounts will be deleted accordingly.

- Employees: Accounts will automatically be created upon active employment with the college. Employment status is defined by the Human Resources Office. These accounts will be disabled immediately upon a written notification from the Human Resources office or lack of use for a period of 120 days. Disabled accounts will be deleted 30 days after account was disabled. User files will be moved to secured network space for department head review.
- Special Users: An Account will be created at the request of a department head and approved by the Vice President of that department and the Director of Computer Services. These accounts will be disabled immediately upon a written notification from the Human Resources office or lack of use for a period of 120 days. Disabled accounts will be deleted 30 days after account was disabled. User files will be moved to secured network space for department head review if applicable.
- ERP/Administrative Systems Accounts: Access to the ERP/Administrative Computer is highly restricted to users with very specific business need. All accounts are created manually. A user must complete the proper security forms and obtain approval from the department head and the Security Coordinator(s) of the administrative system(s) (see appendix A). Access to administrative systems requires access to the network and thus a Network Account is also required. These accounts will be disabled immediately upon a written notification from the Human Resources office or lack of use for a period of 30 days. Disabled accounts will be deleted 90 days after account was disabled. All related Screen Access will be disabled and/or deleted according to the same criteria relating to the ERP Account itself. User files will be moved to secured network space for department head review if applicable.
- All users must read and abide by the Lamar State College - Port Arthur Information Resources Security Acknowledgement and Nondisclosure Agreement before accessing any Information Resource at Lamar State College – Port Arthur.
- Accessing any Lamar State College – Port Arthur Information Resources constitutes acceptance of the Information Resources Use and Security Policies, and hence binds the user by all aspects of these policies.
- All accounts are uniquely identifiable using the assigned user name.
- All passwords for accounts are constructed in accordance with the Lamar State College - Port Arthur Password Policy.
- All accounts have a password expiration that complies with the Lamar State College - Port Arthur Password Policy.
- Accounts of individuals on extended leave (more than 90 days) will be disabled.
- All new user Network accounts that have not been accessed within 120 days of creation will be disabled.
- All user accounts that have not been accessed within 120 days of creation will be deleted.
- System Administrators or other designated staff:
 - ❖ are responsible for removing the accounts of individuals who change roles within Lamar State College - Port Arthur or are separated from their relationship with Lamar State College - Port Arthur

- ❖ must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
- ❖ must have a documented process for periodically reviewing existing accounts for validity
- ❖ are subject to independent audit review
- ❖ must provide a list of accounts for the systems they administer when requested by authorized Lamar State College - Port Arthur management
- ❖ must cooperate with authorized Lamar State College - Port Arthur management investigating security incidents

5.16.11.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 2, 3, 4, 5, 6, 7, 9, 16, and 17 in appendix D.

5.16.12 Administrator/Special Access Policy

5.16.12.1 Introduction

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical student, faculty, or staff users. The fact that these administrative and special access accounts (also known as System Administrator Accounts) have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

5.16.12.2 Purpose

The purpose of the Lamar State College - Port Arthur Administrative/Special Access Practice Policy is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

5.16.12.3 Audience

The Lamar State College - Port Arthur Administrative/Special Access Practice Policy applies equally to all individuals who have, or may require, System Administrator Accounts or certain other special access privilege to any Lamar State College - Port Arthur Information Resources.

5.16.12.4 Policy

- Lamar State College - Port Arthur departments must submit to Computer Services a list of administrative contacts for their systems that are connected to the Lamar State College - Port Arthur network.
- All users must sign the Lamar State College - Port Arthur Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All users of System Administrator or other special access accounts must have account management instructions, documentation, training, and authorization.
- Each individual who uses System Administrator or other special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the ISO.
- Each individual who uses System Administrator or other special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must comply with the Lamar State College - Port Arthur Password Policy.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or Lamar State College - Port Arthur, or upon a change in the third party vendor personnel assigned to a Lamar State College - Port Arthur contract.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
 - ❖ must be authorized
 - ❖ must be created with a specific expiration date

❖ must be removed when work is complete

5.16.12.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 2, 3, 4, 5, 6, 7, 9, 16, and 17 in appendix D.

5.16.13 Password Policy

5.16.13.1 Introduction

User authentication is a means to control who has access to an Information Resource system. Controlling the access is necessary for any Information Resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to Lamar State College - Port Arthur.

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice
- A combination of factors – Smartcard and a PIN

5.16.13.2 Purpose

The purpose of the Lamar State College - Port Arthur Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Lamar State College - Port Arthur user authentication mechanisms.

5.16.13.3 Audience

The Lamar State College - Port Arthur Password Policy applies equally to all individuals who use any Lamar State College - Port Arthur information resource.

5.16.13.4 Policy

- All passwords, including initial passwords, must be constructed and implemented according to the following Lamar State College - Port Arthur IR rules:
 - ❖ it must be routinely changed
 - ❖ it must adhere to a minimum length as established by Lamar State College - Port Arthur Computer Services
 - ❖ it must be a combination of alpha and numeric characters
 - ❖ it must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
 - ❖ it must not be dictionary words or acronyms
 - ❖ password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. Lamar State College - Port Arthur Computer Services personnel and Computer Services contractors will not ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Lamar State College - Port Arthur.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Lamar State College - Port Arthur ISO. In order for an exception to be approved there must be a

procedure to change the passwords.

- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- Computer Services Helpdesk password change procedures must include the following:
 - ❖ authenticate the user to the helpdesk before changing password
 - ❖ change to a strong password
 - ❖ the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
 - ❖ Take control of the passwords and protect them
 - ❖ Report the discovery to the Lamar State College - Port Arthur Help Desk
 - ❖ Transfer the passwords to an authorized person as directed by the Lamar State College - Port Arthur ISO

Password Guidelines

- Passwords must be changed at least every 90 days.
- Passwords must have a minimum length of 8 alphanumeric characters
- Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#\$\$%^&* _+=?/~`.;:,<>|\).
- Passwords must not be easy to guess and they:
 - ❖ must not be your Username
 - ❖ must not be your employee number
 - ❖ must not be your name
 - ❖ must not be family member names
 - ❖ must not be your nickname
 - ❖ must not be your social security number
 - ❖ must not be your birthday
 - ❖ must not be your license plate number
 - ❖ must not be your pet's name
 - ❖ must not be your address
 - ❖ must not be your phone number
 - ❖ must not be the name of your town or city
 - ❖ must not be the name of your department
 - ❖ must not be street names
 - ❖ must not be makes or models of vehicles
 - ❖ must not be slang words
 - ❖ must not be obscenities
 - ❖ must not be technical terms
 - ❖ must not be school names, school mascot, or school slogans
 - ❖ must not be any information about you that is known or is easy to glean (favorite - food, color, sport, etc.)
 - ❖ must not be any popular acronyms
 - ❖ must not be words that appear in a dictionary
 - ❖ must not be the reverse of any of the above
- Passwords must not be reused for a period of one year
- Passwords must not be shared with anyone
- Passwords must be treated as confidential information

Creating a strong password

- Combine short, unrelated words with numbers or special characters. For example:
eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
 - ❖ livefish - is a bad password
 - ❖ L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
 - ❖ !!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable

5.16.13.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 2, 3, 4, 5, 9, 16, and 17 in appendix D.

5.16.14 Portable Computing Policy

5.16.14.1 Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

5.16.14.2 Purpose

The purpose of the Lamar State College - Port Arthur Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of Lamar State College - Port Arthur information.

5.16.14.3 Audience

The Lamar State College - Port Arthur Portable Computing Security Policy apply equally to all individuals who utilize Portable Computing devices and access Lamar State College - Port Arthur Information Resources.

5.16.14.4 Policy

- Only Lamar State College - Port Arthur approved portable computing devices may be used to access Lamar State College - Port Arthur Information Resources.
- Portable computing devices must be password protected.
- Lamar State College - Port Arthur data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive Lamar State College - Port Arthur data must be encrypted using approved encryption techniques.
- Lamar State College - Port Arthur data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- All remote access (dial in services) to Lamar State College - Port Arthur must be either through an approved modem pool or via an Internet Service Provider (ISP).
- Non Lamar State College - Port Arthur computer systems that require network connectivity must conform to Lamar State College - Port Arthur Computer Services Standards and must be approved in writing by the {AGENCY} ISO.
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

5.16.14.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 5, 7, 12, and 20 in appendix D.

5.16.15 Vendor Access Policy

5.16.15.1 Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors; they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to Lamar State College - Port Arthur.

5.16.15.2 Purpose

The purpose of the Lamar State College - Port Arthur Vendor Access Policy is to establish the rules for vendor access to Lamar State College - Port Arthur Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of Lamar State College - Port Arthur information.

5.16.15.3 Audience

The Lamar State College - Port Arthur Vendor Access Policy applies to all individuals who are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

5.16.15.4 Policy

- Vendors must comply with all applicable Lamar State College - Port Arthur policies, practice standards and agreements, including, but not limited to:
 - ❖ Safety Policies
 - ❖ Privacy Policies
 - ❖ Security Policies
 - ❖ Auditing Policies
 - ❖ Software Licensing Policies
 - ❖ Acceptable Use Policies
- Vendor agreements and contracts must specify:
 - ❖ The Lamar State College - Port Arthur information the vendor should have access to
 - ❖ How Lamar State College - Port Arthur information is to be protected by the vendor
 - ❖ Acceptable methods for the return, destruction or disposal of Lamar State College - Port Arthur information in the vendor's possession at the end of the contract
 - ❖ The Vendor must only use Lamar State College - Port Arthur information and Information Resources for the purpose of the business agreement
 - ❖ Any other Lamar State College - Port Arthur information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- Lamar State College - Port Arthur will provide a Computer Services point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide Lamar State College - Port Arthur with a list of all employees working on the contract. The list must be updated and provided to Lamar State College - Port Arthur within 24 hours of staff changes.
- Each on-site vendor employee must acquire a Lamar State College - Port Arthur

identification badge that will be displayed at all times while on Lamar State College - Port Arthur premises. The badge must be returned to Lamar State College - Port Arthur when the employee leaves the contract or at the end of the contract.

- Each vendor employee with access to Lamar State College - Port Arthur sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate Lamar State College - Port Arthur personnel.
- If vendor management is involved in Lamar State College - Port Arthur security incident management the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable Lamar State College - Port Arthur change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Lamar State College - Port Arthur management.
- All vendor maintenance equipment on the Lamar State College - Port Arthur network that connects to the outside world via the network, telephone line, or leased line, and all Lamar State College - Port Arthur IR vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the Lamar State College - Port Arthur Password Practice Standard and Admin/Special Access Practice Standard. Vendor's major work activities must be entered into a log and available to Lamar State College - Port Arthur management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Lamar State College - Port Arthur or destroyed within 24 hours.
- Upon termination of contract or at the request of Lamar State College - Port Arthur, the vendor will return or destroy all Lamar State College - Port Arthur information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of Lamar State College - Port Arthur, the vendor must surrender all Lamar State College - Port Arthur Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Lamar State College - Port Arthur management.
- Vendors are required to comply with all State and Lamar State College - Port Arthur auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to Lamar State College - Port Arthur must be properly inventoried and licensed.

5.16.15.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 2, 3, 4, 5, 6, 7, 9, 16, and 17 in appendix D.

5.16.16 Backup Policy

5.16.16.1 Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

5.16.16.2 Purpose

The purpose of the Lamar State College - Port Arthur Backup Security Policy is to establish the rules for the backup and storage of electronic Lamar State College - Port Arthur information.

5.16.16.3 Audience

The Lamar State College - Port Arthur Backup Security Policy applies to all individuals within the Lamar State College - Port Arthur enterprise who are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security, and data owners.

5.16.16.4 Services

Computer Services may have existing contracts for offsite backup data storage. These services can be extended to all Lamar State College - Port Arthur entities upon request.

5.16.16.5 Policy

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The Lamar State College - Port Arthur Information Resources backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage, if any, for Lamar State College - Port Arthur must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations, if any, must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest Lamar State College - Port Arthur sensitivity level of information stored.
- A process must be implemented to verify the success of the Lamar State College - Port Arthur electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Signature cards held by the offsite backup storage vendor(s), if any, for access to Lamar State College - Port Arthur backup media must be reviewed annually or when an authorized individual leaves Lamar State College - Port Arthur.
- Procedures between Lamar State College - Port Arthur and the offsite backup storage vendor(s), if any, must be reviewed at least annually.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
 - ❖ System name
 - ❖ Creation Date
 - ❖ Sensitivity Classification [Based on applicable electronic record retention

- regulations.]
- ❖ Lamar State College - Port Arthur Contact Information

5.16.16.6 Supporting Information

This Policy is supported by the following Security Policy Standards references 7, 9, 11, 14, 16, 17, 18, and 19 in appendix D.

5.16.17 Virus Protection Policy

5.16.17.1 Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Some of the actions that can be taken to reduce the risk and drive down the cost of security incidents are implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents

5.16.17.2 Purpose

The purpose of the Computer Virus Protection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

5.16.17.3 Audience

The Lamar State College - Port Arthur Computer Virus Protection Policy applies equally to all individuals who use any Lamar State College - Port Arthur Information Resources.

5.16.17.4 Policy

- All workstations whether connected to the Lamar State College - Port Arthur network, or standalone, must use the Lamar State College - Port Arthur Computer Services approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each file server attached to the Lamar State College - Port Arthur network must utilize Lamar State College - Port Arthur Computer Services approved virus protection software and setup to detect and clean viruses that may infect file shares.
- Each E-mail gateway must utilize Lamar State College - Port Arthur Computer Services approved e-mail virus protection software and must adhere to the Computer Services rules for the setup and use of this software.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.

5.16.17.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 6, 7, 16, 21, and 22 in appendix D.

5.16.18 System Development Policy

5.16.18.1 Introduction

The risk of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Some of the actions that can be taken to reduce the risk and drive down the cost of security incidents are implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents.

5.16.18.2 Purpose

The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software in the Lamar State College - Port Arthur Information Resources.

5.16.18.3 Audience

The Lamar State College - Port Arthur System Development Policy applies equally to all individuals who use any Lamar State College - Port Arthur Information Resources.

5.16.18.4 Policy

- Computer Services is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for Lamar State College - Port Arthur system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical Lamar State College - Port Arthur information.
- All production systems must have designated Owners and Custodians for the critical information they process. Computer Services will perform periodic risk assessments of production systems to determine whether the controls employed are adequate.
- All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) must be assigned for all production systems.
- Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

5.16.18.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 8, 10, 11, 14, and 17 in appendix D.

B. Information Resources Use Policies

5.16.19 Acceptable Use Policy

5.16.19.1 Introduction

Under the provisions of the Information Resources Management Act, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources.

5.16.19.2 Purpose

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

5.16.19.3 Audience

The Lamar State College - Port Arthur Acceptable Use policy applies equally to all individuals granted access privileges to any Lamar State College - Port Arthur Information Resources.

5.16.19.4 Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of Lamar State College - Port Arthur are the property of Lamar State College - Port Arthur.

5.16.19.5 Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of Lamar State College - Port Arthur are not private and may be accessed by Lamar State College - Port Arthur Information Resources Security personnel at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

5.16.19.6 Policy

- Users must report any weaknesses in Lamar State College - Port Arthur computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on Lamar State College - Port Arthur systems for which they do not have authorization or explicit consent.
- Users must not divulge dialup or dial back modem phone numbers to anyone.
- Users must not share their Lamar State College - Port Arthur account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. Users must not make unauthorized copies of copyrighted software.

- Users must not use non-standard shareware or freeware software without Lamar State College - Port Arthur Information Resources management approval unless it is on the Lamar State College - Port Arthur standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized Lamar State College - Port Arthur user access to a Lamar State College - Port Arthur resource; obtain extra resources beyond those allocated; circumvent Lamar State College - Port Arthur computer security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Lamar State College - Port Arthur users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Lamar State College - Port Arthur Information Resources.
- Lamar State College - Port Arthur Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which Lamar State College - Port Arthur may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the Lamar State College - Port Arthur official processes for dealing with academic ethical issues).
- Access to the Internet from a Lamar State College - Port Arthur owned, home based, computer must adhere to all the same policies that apply to use from within Lamar State College - Port Arthur facilities. Employees must not allow family members or other non-employees to access Lamar State College - Port Arthur computer systems.
- Users must not otherwise engage in acts against the aims and purposes of Lamar State College - Port Arthur as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use

As a convenience to the Lamar State College - Port Arthur user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, etc., is restricted to Lamar State College - Port Arthur approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Lamar State College - Port Arthur.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, Lamar State College - Port Arthur.
- Storage of personal email messages, voice messages, files and documents within Lamar State College - Port Arthur's Information Resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on Lamar State College - Port Arthur Information Resources are owned by Lamar State College - Port Arthur, may be subject to open records requests, and may be accessed in accordance with this policy.

This Policy is supported by the following Security Policy Standards references 3, 6, 7, 8, 16, 21, and 22 in appendix D.

5.16.20 Internet Policy

5.16.20.1 Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources.

5.16.20.2 Purpose

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the internet.
- To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

5.16.20.3 Audience

The Lamar State College - Port Arthur Internet Use Policy applies equally to all individuals granted access to any Lamar State College - Port Arthur Information Resource with the capacity to access the internet, the intranet, or both.

5.16.20.4 Ownership

Electronic files created, sent, received, or stored on computers owned, leased administered, or otherwise under the custody and control of Lamar State College - Port Arthur are the property of Lamar State College - Port Arthur.

5.16.20.5 Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of Lamar State College - Port Arthur are not private and may be accessed by Lamar State College - Port Arthur Computer Services employees at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

5.16.20.6 Policy

- Software for browsing the Internet is provided to authorized users for business and research use only.
- All software used to access the Internet must be part of the Lamar State College - Port Arthur standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.
- Only the Lamar State College - Port Arthur Computer Services Department and its designees shall establish standards and coding of departmental pages or documents for the World Wide Web (WWW) servers owned and operated by the College.
- All files downloaded from the Internet must be scanned for viruses using the approved Computer Services distributed software suite and current virus detection software.
- All software used to access the Internet shall be configured to use the firewall and possibly an http proxy.
- All sites accessed must comply with the Lamar State College - Port Arthur Acceptable

Use Policies.

- All user activity on Lamar State College - Port Arthur Information Resources assets is subject to logging, monitoring, and review.
- Content on all Lamar State College - Port Arthur Web sites must comply with the Lamar State College - Port Arthur Acceptable Use Policies.
- No offensive or harassing material may be made available via Lamar State College - Port Arthur Web sites.
- Material that might be considered abusive, indecent, harassing, or threatening may be accessed, activated, and viewed only insofar as those materials and resources are required to perform legitimate job functions. However, caution must be exercised to avoid displaying the material in any way that might interfere with the performance of other employees or that creates an abusive, intimidating, harassing, hostile, or threatening workplace or academic environment.
- Non-business related purchases made over the internet are prohibited. Business related purchases are subject to Lamar State College - Port Arthur procurement rules.
- No personal commercial advertising may be made available via Lamar State College - Port Arthur Web sites.
- Lamar State College - Port Arthur internet access may not be used for personal gain or non-Lamar State College - Port Arthur personal solicitations.
- No Lamar State College - Port Arthur data will be made available via Lamar State College - Port Arthur Web sites without ensuring that the material is available to only authorized individuals or groups.
- All sensitive Lamar State College - Port Arthur material transmitted over external network must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.
- Using the College's Internet connection to access other computer systems in violation of the policies of the entity that owns those systems is strictly prohibited.
- Illegal material may not be used to perform any legitimate job function and therefore may not be accessed, viewed, or stored on College computing facilities.

Incidental Use

- Incidental personal use of Internet access is restricted to Lamar State College - Port Arthur approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Lamar State College - Port Arthur.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to, Lamar State College - Port Arthur.
- Storage of personal files and documents within Lamar State College - Port Arthur's Information Resources should be nominal.
- All files and documents – including personal files and documents – are owned by Lamar State College - Port Arthur, may be subject to open records requests, and may be accessed in accordance with this policy.

5.16.20.7 Supporting Information

This Policy is supported by the following Security Policy Standards references 3, 6, 7, and 16 in appendix D.

5.16.21 E-Mail Policy

5.16.21.1 Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of E-Mail.
- To educate individuals using E-Mail with respect to their responsibilities associated with such use.

5.16.21.2 Purpose

The purpose of the Lamar State College - Port Arthur E-Mail Policy is to establish the rules for the use of Lamar State College - Port Arthur E-Mail for the sending, receiving, or storing of electronic mail.

5.16.21.3 Audience

The Lamar State College - Port Arthur E-Mail Policy applies equally to all individuals granted access privileges to any Lamar State College - Port Arthur information resource with the capacity to send, receive, or store electronic mail.

5.16.21.4 Policy

- The following activities are prohibited by policy:
 - ❖ Sending E-Mail that is intimidating or harassing.
 - ❖ Using E-Mail for conducting personal business.
 - ❖ Using E-Mail for purposes of political lobbying or campaigning.
 - ❖ Violating copyright laws by inappropriately distributing protected works.
 - ❖ Posing as anyone other than oneself when sending E-Mail, except when authorized to send messages for another when serving in an administrative support role.
 - ❖ The use of unauthorized e-mail software.
- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - ❖ Sending or forwarding chain letters.
 - ❖ Sending unsolicited messages to large groups except as required to conduct agency business.
 - ❖ Sending excessively large messages
 - ❖ Sending or forwarding E-Mail that is likely to contain computer viruses.
- All sensitive Lamar State College - Port Arthur material transmitted over external network must be encrypted.
- All user activity on Lamar State College - Port Arthur Information Resources assets is subject to logging, monitoring, and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Lamar State College - Port Arthur or any unit of the Lamar State College - Port Arthur unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the Lamar State College - Port Arthur. An example of a simple disclaimer is: "the opinions

expressed are my own, and not necessarily those of my employer."

- Individuals must not send, forward or receive confidential or sensitive Lamar State College - Port Arthur information through non-Lamar State College - Port Arthur E-Mail accounts. Examples of non-Lamar State College - Port Arthur E-Mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and E-Mail provided by other Internet Service Providers (ISP).
- Individuals must not send, forward, receive or store confidential or sensitive Lamar State College - Port Arthur information utilizing non-Lamar State College - Port Arthur accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.
- The same standards of conduct expected of users regarding the use of telephones, libraries, and other College resources apply to the use of electronic messaging. Users will be held no less accountable for actions in situations involving electronic messaging than when dealing with other media.
- Any communication where the meaning of the message, or its transmission or distribution, would be illegal, unethical, or irresponsible is to be avoided.

5.16.21.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 3, 6, 7, and 8 in appendix D.

5.16.22 Instant Messaging Policy

5.16.22.1 Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of Instant Messaging.
- To educate individuals using Instant Messaging with respect to their responsibilities associated with such use.

5.16.22.2 Purpose

The purpose of the Lamar State College - Port Arthur Instant Messaging Policy is to establish the rules for the use of Lamar State College - Port Arthur Instant Messaging for the sending, receiving, or storing of Instant Messages.

5.16.22.3 Audience

The Lamar State College - Port Arthur Instant Messaging Policy applies equally to all individuals granted access privileges to any Lamar State College - Port Arthur information resource with the capacity to send, receive, or store instant messages.

5.16.22.4 Policy

- Employees will not download/install any Instant Messaging (IM) software without specific authorization in writing from the Lamar State College – Port Arthur Director of Computer Services.
- Employees authorized to use IM technologies will not download any illegal and/or unauthorized copyrighted content. The Director of Computer Services must approve the use of IM technology to download copyrighted material in writing. The state entity must follow appropriate state and federal laws and guidelines when copying, storing, or transferring copyrighted material.
- This policy applies to IM used within the agency or institution and IM used conjointly with the Internet and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, IM should be used only for legitimate state business; however, brief and occasional IM of a personal nature may be sent and received if the following conditions are met.
- Personal use of IM is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.
- Authorized state network users should keep in mind that all IM can be recorded and stored along with the source and destination. Users have no right to privacy with regard to IM. Management has the ability and right to view employees' IM. Recorded instant messages are the property of Lamar State College – Port Arthur. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

- Incidental amounts of employee time, time periods comparable to reasonable coffee breaks during the day, can be used to attend to personal matters via IM or other telecommunications, similar to personal telephone calls.
- Personal IM should not impede the conduct of state business.
- If authorized for usage on state systems, IM may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.
- Do not use IM to conduct any state business that would require the content to be saved as a state record. IM may not be used to document a statutory obligation or agency decision, and IM should not be used when the resulting record would normally be retained for recordkeeping purposes.
- Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.
- IM should not be used for any personal monetary interests or gain.

5.16.22.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 3, 6, 7, and 8 in appendix D.

5.16.23 Peer-to-Peer (P2P) Policy

5.16.23.1 Introduction

Under the provisions of the Information Resources Management Act and [Executive Order \(RP58\) Relating to peer-to-peer file-sharing software](#), information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of Peer-to-Peer software.
- To educate individuals using Peer-to-Peer technology with respect to their responsibilities associated with such use.

5.16.23.2 Purpose

The purpose of the Lamar State College - Port Arthur Peer-to-Peer Policy is to establish the rules for the appropriate use of Peer-to-Peer software at Lamar State College - Port Arthur.

5.16.23.3 Audience

The Lamar State College - Port Arthur Peer-to-Peer Policy applies equally to all individuals granted access privileges to any Lamar State College - Port Arthur information resource with the capacity to send, receive, or store electronic mail.

5.16.23.4 Policy

- This policy applies to Peer-to-Peer (P2P) used within Lamar State College – Port Arthur and P2P used conjointly with the Internet and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, P2P should be used only for legitimate state business; however, brief and occasional P2P of a personal nature may be sent and received if the following conditions are met.
- Users of state computers or networks that are authorized to use P2P technologies will not download any illegal and/or unauthorized copyrighted content. The Director of Computer Services must approve the use of P2P technology to download copyrighted material in writing. State users must follow appropriate state and federal laws and guidelines when copying, storing, or transferring copyrighted material.
- If authorized for usage on state systems, P2P may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.
- Users of state computers or networks shall not download/install or use any P2P software on state computers, networks, or mobile computing device (PDA) without specific authorization in writing from the Director of Computer Services.
- Personal use of P2P is a privilege that must be granted specifically in writing by the Director of Computer Services. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.
- Authorized network users may use P2P technologies for official business only if specifically authorized in writing by the Director of Computer Services.

- If any copied or transferred data or information is licensed or copyrighted, the Director of Computer Services and authorized network user shall ensure that all notifications and costs are documented and approved.
- Users of state computers and networks should keep in mind that all P2P may be recorded and stored along with the source and destination. Employees have no right to privacy with regard to P2P. Management has the ability and right to view users' P2P on state systems.
- P2P files recorded on state systems are the property of Lamar State College – Port Arthur. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.
- If authorized in writing by the Director of Computer Services, incidental amounts of employee time, time periods comparable to reasonable coffee breaks during the day, may be used to attend to personal matters via P2P, similar to personal telephone calls. Personal P2P use should not cause the state to incur a direct cost in addition to the general overhead of an Internet connection; consequently, users are not permitted to print or store personal electronic files or material on a state network.
- Personal P2P use should not impede the conduct of state business; only incidental amounts of employee time, time periods comparable to reasonable coffee breaks during the day, should be used to attend to personal matters.
- Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.
- P2P should not be used for any personal monetary interests or gain.

5.16.23.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 3, 6, 7, and 8 in appendix D.

5.16.24 Software Licensing Policy

5.16.24.1 Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

5.16.24.2 Purpose

The purpose of the Software Licensing Policy is to establish the rules for licensed software use on Lamar State College - Port Arthur Information Resources.

5.16.24.3 Audience

The Lamar State College - Port Arthur Software Licensing Policy applies equally to all individuals who use any Lamar State College - Port Arthur owned/licensed software.

5.16.24.4 Policy

- Lamar State College - Port Arthur provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information or software, that Lamar State College - Port Arthur does not have specific approval to store and/or use, must not be stored on Lamar State College - Port Arthur systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).
- Third party software in the possession of Lamar State College - Port Arthur must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes. Manuals, and other copyrighted materials, shall not be copied without specific, written permission of the publisher.
- Permission is granted to users for the use of licensed software according to the regulations set forth herein by Lamar State College - Port Arthur for the use of such software. The use of such software is governed by the terms of licensing agreements between the College and the software licensors, and the user must read and abide by the terms of those agreements.
- Computer software shall be used in strict accordance to its licensing agreement. By way of example only, such agreements may prohibit the copying of software from one computer to another or the making of unauthorized copies to install on computers not owned or controlled by the College.
- Most software is proprietary and may therefore be subject to copyright or patent restrictions as defined in the license agreements.

- Users may make only one backup copy of the software for archival purposes. If the underlying license is discontinued, this copy must be destroyed. Otherwise, users must not copy, disclose, transfer, or remove any proprietary programs from the media on which the software resides.
- Users must not use Lamar State College - Port Arthur equipment or software to violate the terms of any software license agreement. Information on specific software licenses on all public computer systems can be obtained from the Computer Services Department.
- Software for which the College holds the license may not be copied or removed from a College-owned computer and placed on another College-owned computer or any computer owned by any other person or entity.
- Ordinarily, the College must own or hold the license for any software loaded onto a College-owned computer.
- An individual user may request that the Computer Services Department install software that, while not purchased or licensed by the College, the user can utilize for business or instructional purposes. In this case the user must demonstrate or certify the purchase or license of the software. The decision to load software that is not owned by the College rests with the Director of Computer Services.
- The Computer Services Department reserves the right to audit any personal computer on College property-regardless of whether or not the equipment is owned, operated, or controlled by the College-at any time for unauthorized software.
- These rules also govern shareware and freeware programs that can be obtained from Internet access. All programs coming from Internet sources must be approved for use and be installed by the Computer Services Department.
- All software should be scanned for viruses before use.
- Standardized Internet access software such as browsers, graphics converters, etc. shall be provided by the Computer Services Department. These programs will have been tested and found to be virus free.
- Software loaded on College-owned computers must support the mission of the College and should have the primary purpose of assisting the user to perform legitimate job functions.
- The Computer Services Department shall load all software on all equipment for which it has direct responsibility. The Computer Services Department shall not support any software that it did not install and shall not install software that it feels it cannot adequately support.
- Lamar State College - Port Arthur software applications shall not be used to create, modify, access, view, display, or activate files, information, or materials that are offensive, indecent, or illegal.
- Each manufacturer includes a license agreement package with its software that details any restrictions on its use. Users must comply with the vendor's license provisions

regarding the use of the software, even though the individual user has not personally signed the license agreement. License agreements differ among the various software vendors and some may grant additional rights, such as allowing use on a portable or home computer. The College shall hold each user responsible for reading, understanding, and complying with provisions of the license agreement for each software package.

5.16.24.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 8, 9, and 21 in appendix D.

5.16.25 Computing Facilities Use Policy

5.16.25.1 Introduction

The computing facilities at Lamar State College - Port Arthur are provided for the support of the programs of the College. All users are responsible for seeing that these facilities are used solely for the transaction of College business in an effective, efficient, ethical, and lawful manner. Any use of these facilities in any way other than those stated below will be considered in violation of College policy.

5.16.25.2 Purpose

The purpose of the Computing Facilities Use Policy is to establish the rules, guidelines, and expectations for the use of computing facilities at Lamar State College - Port Arthur.

5.16.25.3 Audience

The Lamar State College - Port Arthur Computing Facilities Use Policy applies equally to all individuals who use any Lamar State College - Port Arthur computing facilities.

5.16.25.4 Policy

- Users shall be accountable for using computing facilities in an effective, ethical and lawful manner.
- Users must not use Lamar State College - Port Arthur's computer systems, including any of its communications facilities and services, in any way which deliberately diminishes or interferes with the reasonable and confidential use of those systems for College business by others, or which is intended to do the same. Lamar State College - Port Arthur retains the right to access and remove immediately any data or files evidencing any such misuse.
- The Computer Services Department must approve all access to the College's central computer systems. Department heads must approve all access to computer systems under their direct control.
- Account access information assigned to an individual for use of the central computers or departmental systems is not to be given to another individual. The individual assigned an account is responsible for all activity for which that account is used. Use of another person's account is not only a violation of College policy; it is a violation of state law.
- Computing facilities and accounts are owned by the College and are to be used for College-related activities only.
- Users are expected to abide by the security restrictions on all systems and information to which they have access.
- Programs and files are confidential, and may only be accessed by those persons authorized to do so.

- Please be sensitive to the inherent limitations of shared network resources. No computer security system can prevent a determined person from gaining unauthorized access to stored information. Good judgment dictates the creation of electronic documents that, should they become available to the public, will not bring embarrassment or liability to the College or its constituencies.
- Use of College computing facilities to create, display, modify, or transmit files that are abusive, harassing, threatening, indecent, or illegal is expressly prohibited.
- Material that might be considered indecent, abusive, harassing, or threatening may be accessed, activated, and viewed only insofar as those materials and resources are required to perform legitimate job functions. However, caution must be exercised to avoid displaying the material in any way that might interfere with the performance of other employees or that creates an intimidating, hostile, or offensive workplace or academic environment.
- Illegal material may not be used to perform any legitimate job function and therefore may not be accessed, viewed, or stored on College computing facilities.
- Users are expected to promote efficient use of network resources consistent with the instructional, research, public service and administrative goals of the College. Users must display consideration for others and refrain from engaging in any use that would interfere with their work or disrupt the intended use of network resources. Wasteful and disruptive practices such as sending chain letters, broadcast messages or unwanted material are specifically prohibited.
- Conduct that involves the use of computing or communications resources to violate a College policy or regulation, or to violate another's rights, is a serious abuse and can result in limitation of privileges and lead to appropriate disciplinary action.

5.16.25.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 8, 9, and 21 in appendix D.

5.16.26 Telephone Systems Policy

5.16.26.1 Introduction

The Lamar State College -Port Arthur telephone systems and facilities are intended to support the academic mission and the administrative functions of the College.

5.16.26.2 Purpose

The purpose of the Computing Telephone Systems Use Policy is to establish the rules, guidelines, principles, and expectations for the use of the telephone systems at Lamar State College - Port Arthur.

5.16.26.3 Audience

The Lamar State College - Port Arthur Telephone Systems Use Policy applies equally to all individuals who use any Lamar State College - Port Arthur telephone systems.

5.16.26.4 Policy

- Users are accountable for using these facilities and equipment in an effective, ethical, and lawful manner.
- Users must only use these facilities and equipment for which they have authorization, whether these facilities are at Lamar State College - Port Arthur or at any other facility which is accessible through the Lamar State College – Port Arthur telephone systems.
- Users must take all reasonable steps to protect the privacy of others as well as the integrity of Lamar State College - Port Arthur. Users shall not share with others PIN numbers, passwords, or any other authorization which has been assigned to them.
- Telephones should be used for business purposes only except in case of emergency. All long distance calls not specifically for business purposes should be charged to the user's personal account.
- Users must be aware that all calls data are monitored by a call detail recording system located in the Data Center. These reports are available to the President, Vice President of Academic Affairs, and Director of Computer Services as needed to insure proper use, and are available to other supervisors upon written request.
- Maintenance, monitoring, and reporting of these principles are the responsibility of the Director of Computer Services. Any violation of the Policy may result in disciplinary action in accordance with College policies.

5.16.26.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 1, 3, 8, 9, and 21 in appendix D.

VI. Appendices

Appendix A: Administrative Systems Assets/Custodians

The following table is a list of Lamar State College - Port Arthur's administrative information systems (software and data assets) together with the custodian of each system. Information system assets not listed here are departmentally administered and each asset is the responsibility of the Manager having custody of the asset. The list is assigned and approved by the President of LSCPA (documentation available).

| Asset Name/Application | Asset Description | Asset Custodian |
|------------------------|---|--|
| SunGard H.E. PLUS FRS | Financial Records System, Purchasing, Accounts Payable, BDS (budget) and Interfaces Systems | VP for Finance |
| SunGard H.E. PLUS HRS | Human Resources System, Personnel, Payroll, Position Control/Budget Systems | Human Resources Director, Payroll Director, Associate VP for Finance |
| SunGard H.E. PLUS SIS | Student Information Systems - Student Records, Admission, Financial Aid Systems | VP for Student Services |
| SunGard H.E. PLUS SIS | Student Information System Billing and Receivables System | VP for Finance |

Appendix B: Information Resources Policies Maintenance

The maintenance of this Manual will be the responsibility of the Director of Computer Services. This document will be reviewed annually. Changes will be made to the Manual as necessitated by federal and state laws as well as changes in the College policies. All changes will be approved by the President prior to adoption.

Notices of any changes to the Manual will be disseminated campus-wide and posted to the college web site.

Appendix C: Definitions

The following are definitions of terms used in the Information Resources Policies:

Access: To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

Access Control: The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Administrative Application: An assortment of computer software that works together to support administrative operations and activities for one or more departments. Examples include: the Student Information System, the Human Resource System, and the Financial Records System. Applications that exist primarily to support research and teaching activities are not included in the definition.

Agent: The organizational unit providing technical facilities, software development, data processing, telecommunications, printing and support services to custodians and users of automated information. Agent responsibility resides with any person or group charged with the physical possession or control of information assets by custodians and College management. Agents are charged with satisfying the custodian's requirements for processing, telecommunications, protection controls, and output distribution of the resource.

Authentication: The process that verifies the claimed identity of a station, originator, or individual as established by the identification process.

Authorization: Positive determination by the custodian of an information resource that a specific individual or system may access that information resource, or validation that a positively identified user has the need and the custodian's permission to access the resource.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

Centrally Administered Computer System {WAN, LAN, Lab}: The computing hardware, software, and communications network that comprise any system {WAN, LAN, lab} that is under the direct management of the Computer Services Department. Centrally administered {systems, LANs, labs} are generally accessible to and shared by the entire campus community and are rarely dedicated to the exclusive use of any single functional component of the College. Centrally Administered Computer System {WAN, LAN, Lab}: The computing hardware, software, and communications network that comprise any system {WAN, LAN, lab} that is under the direct management of the Computer Services Department. Centrally administered {systems, LANs, labs} are generally accessible to and shared by the entire campus community and are rarely dedicated to the exclusive use of any single functional component of the College.

Change can consist of any or all of the following:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Computer Services (CS): The name of the agency department responsible for computers, networking and data management.

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization

Confidential Information: Information maintained by the College that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws. Examples of confidential records include personnel records, transcripts, grades, grade point averages, test scores, academic and disciplinary status, health information, personal and family financial information, and placement file recommendations and ratings.

Critical Information Resource: A resource determined by the College's executive management to be essential to the College's critical mission and functions, the loss of which would have an unacceptable impact, as identified through appropriate risk analysis activities.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Computer Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Data: A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

Data Integrity: The state that exists when computerized information is predictably related to its source and has been subjected to only those processes which have been authorized by the appropriate personnel.

Data Security (or Computer Security): Those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.

Departmentally Administered Computer System (WAN, LAN, Lab): The computing hardware, software and communications network that comprise any system that is under the direct management of any single College organization other than Computer Services. Departmentally administered {systems, LANs, labs} are not generally shared outside the department and are routinely dedicated to the exclusive use of a single functional component of the College.

Disaster: A condition in which a critical information resource is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the College's mission or critical functions.

Disclosure: User right to access government records. All government information is presumed to be available to the public. Certain exceptions may apply to the disclosure of the information. Governmental bodies shall promptly release requested information that is not confidential by law or information for which an exception to disclosure has been sought.

Email Account: A class of computer account that provides limited access to the My.Lamarpa.edu web based portal and includes an email address hosted by the college. It does not provide access to personal computers owned by Lamar State College – Port Arthur or any network resources other than the web portal and email address.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Encryption: The process of cryptographically converting plain text electronic data into a form unintelligible to anyone other than the originator and the intended recipient.

ERP Account: A class of computer account that provides limited access to one or more parts of the Enterprise Resource Planning Software used by Lamar State College – Port Arthur.

Exposure: Vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.

Firewall: An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Host: A computer system that provides computer service for a number of users.

Information: That which is extracted from a compilation of data in response to a specific need.

Information Attack: An attempt to bypass the physical or information security measures and controls protecting any Information Resources System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information super highway."

Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually

protected from external access by a firewall.

Local Area Network (LAN): The linkage of computers and other devices within a limited area to facilitate electronic communication, information sharing, and shared access to peripheral equipment.

Manager: An administrative head or account manager who is responsible and accountable for the activities conducted in one or more organizational units or facilities within the College, and for the information resources used in conducting those activities.

Network Account: Is defined as a class of computer account that provides limited access to personal computers and network resources owned by Lamar State College – Port Arthur. When both Network and Email Accounts are provided, the passwords are automatically synchronized.

Offsite Storage: Based on data criticality, offsite storage should be in a geographically different location from the Lamar State College - Port Arthur campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building containing the original data and storing it in another secured location on the Lamar State College - Port Arthur Campus may be appropriate.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

PIN: is an acronym for Personal Identification Number. It is commonly used to access secure computer systems and/or facilities.

A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

Privacy: Privacy is the principle, as defined under federal, state, or agency rules, which sets the boundaries for personal scrutiny or exposure. Privacy secures data that is defined by federal, state or agency rules as private or protected, or deemed exempt under Chapter 552. Organizations need to secure public information according to the threat and impact of disclosure. Additionally, users should expect that data, other than that deemed private or protected by applicable law, be subject to examination by authorized users or through open records requests.

Risk: The likelihood or probability that a loss of information resources or breach of security will occur.

Risk Analysis: Is defined as an evaluation of system assets and their vulnerabilities to threats. Risk analysis estimates potential losses that may result from threats.

Risk Management: Are decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Officer, technical management may designate a number of security administrators.

Security Controls: Hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of information and the means of processing it.

Security Incident (or Breach): In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Sensitive Information: Information maintained by the College that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness.

Server: A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the owner such as a birth date, social security number, etc.

System Administrator: Person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce an organization's security policy.

System Administrator Account: A class of computer account that provides unlimited access to a particular Information Resource asset or group of assets. These accounts are used to effectively manage the Information Resource and their distribution is strictly controlled.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.

User: The user is any person who has been granted one or more Lamar State College – Port Arthur computer accounts. The user has the responsibility to comply with all policies and procedures adopted by Lamar State College – Port Arthur. The user is the single most effective control for providing adequate security. A user has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Username: A data item associated with a specific individual which represents the identity of that individual and may be known by other individuals.

Vendor: someone who exchanges goods or services for money.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

Web server: A computer that delivers (*serves up*) web pages.

Website: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) and which may contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Appendix D: Standard Policy Statements

The following are Standard Policy Statements that support the Information Resources Policies.

1. IR Security controls must not be bypassed or disabled.
2. Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3. All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
4. Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management.
5. Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
6. The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management
7. Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
8. All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.
9. On termination of the relationship with the agency users must surrender all property and IR managed by the agency. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
10. The owner must engage the IRM, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with the agency authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published.
11. The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired

for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.

12. The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
13. The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all agency legal and fiscal policies and procedures.
14. The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.
15. All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.
16. Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.
17. All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.
18. All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized Lamar State College - Port Arthur officer and must contain terms approved as to form by the Legal Department, advising vendors of Lamar State College - Port Arthur's IR retained proprietary rights and acquired rights with respect to its information systems, programs, and data requirements for computer systems security, including data maintenance and return.
19. Lamar State College - Port Arthur IR computer systems and/or associated equipment used for Lamar State College - Port Arthur business that is conducted and managed outside of Lamar State College - Port Arthur control must meet contractual requirements and be subject to monitoring.
20. External access to and from IR must meet appropriate published agency security guidelines.
21. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IS reserves the right to remove any unlicensed software from any computer system.
22. The IRM through IS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

Appendix E: Software/Hardware Selection, Budgeting, and Acquisition

The Director of Computer Services must approve all software and hardware purchases. The Computer Services Department will conduct all quotes for bids and prices. Each division, department, and office should consult with the Computer Services Department when preparing its annual budget for assistance in developing its requests for funds for hardware and software acquisitions.