working days. The writing sample will be graded off-site and will take approximately five days.

Complaints, Grievances and Appeals: The goal is to provide equitable, timely, fair and accurate resolutions to problems and complaints. Initial complaints or problems should be brought to the attention of the relevant department for resolution. If an acceptable resolution is not reached within five working days, the student can then file a formal written complaint. If a student wishes to file a formal complaint, the process and procedures for filing a written complaint, grievance or appeal is available through The Texas State University System Rules and Regulations, the LSC-PA Student Handbook, the Faculty Handbook, the college catalog and/or website.

Student Relations Representative: Dr. Gary Stretcher, Vice President for Academic Affairs, Lamar State College-Port Arthur, P.O. Box 310, Port Arthur, Texas 77641-0310. Phone (409) 984-6209 and fax (409) 984-6000. E-mail: *Gary.Stretcher@lamarpa.edu*. Additional contacts for student relations include the President, the Vice President for Finance and the Vice President for Student Services.

Student Rights and Responsibilities

Academic Dishonesty

In an attempt to clarify possible misunderstandings, LSCPA faculty and staff have developed some definitions and examples of two types of academic dishonestly: cheating and plagiarism. Cheating is defined as the giving or taking of information or material with the purpose of wrongfully aiding oneself or another person in academic work that is to be considered in determining a grade.

Plagiarism, or literary theft, is defined as appropriating the literary composition of another person, including the parts, passages, or language of that writing, and passing off the appropriate material as one's own. Plagiarism is the failure to give proper credit or citation to one's sources(s) of information. It includes the failure to use conventional methods of documentation for material quoted or paraphrased. Additionally, plagiarism includes allowing someone else to compose or rewrite an assignment for a student. Some examples of cheating and/or plagiarism include, but are not limited to, the following items:

1. Asking for or giving another student information during a test;
2. Copying answers from another student's paper or intentionally allowing someone to copy from one's own paper during a test;
3. Using materials prohibited by the instructor during a test;
4. Either impersonating another student during a test or having another person assume one's identity during a test.
5. Changing answers on a previously graded test in order to have a grade revised;
6. Stealing examination materials.
7. Copying material, either exactly or in essence, and not providing appropriate documentation;
8. Copying or falsifying a laboratory or clinical project/assignment, including computer pro- grams, in either disk or hard copy form;
9. Allowing someone else to compose or rewrite a student's assignment;
10. Stealing, buying, selling, or otherwise providing research papers.

As with other violations of student conduct, cheating and/or plagiarism may result in disciplinary action.

Penalty for False Statements

A student who provides false information or makes false statements to any college official or office or on an official form submitted to the College is subject to immediate dismissal.

Computer Services Department Policies

The use of the college's computing and electronic communication resources is a privilege, not a right. That privilege can be revoked at any time if a user violates policies outlined here and contained in detail on the college website at: *www.lamarpa.edu/gen/ir_use_policy.html*.

The Information Resource Use Policy is designed to ensure the ethical, efficient, effective and lawful use of computer hardware, software, networks and systems. Students who violate the policy will receive appropriate disciplinary action from the College and may also face legal action from civil authorities.

No provision of the college's policy supersedes or limits any state or federal laws, or any other Texas State University System or Lamar State College-Port Arthur policies regarding confidentiality, information dissemination or standards of conduct.

The College is committed to:

* Providing students with the computer hardware and software necessary to perform their instructional assignments;

* Protecting its computer environment from viruses;

* Maintaining compliance with the U. S. copyright laws and software license agreement and;

* Discouraging and monitoring for copyright infringement.

Each user is granted non-commercial use of the computing and communications facilities and services of the College according to rules that may be posted at those facilities, and to the terms described in this publication. A student who illegally duplicates software and/or its documentation, violates the policies of the Information Resources Use Policy or otherwise fail to comply with the college's third-party software license agreements, will be subject to disciplinary action up to and including expulsion from school.

Computing Facilities Use Policies:

The college's computing facilities are provided for the support of college programs. All users are responsible for seeing that these facilities are used only for transaction of college business. Computing facilities and accounts are owned by the College and may be used only for college-related activities.

The College reserves the right to allocate and restrict access to computing resources. Users may not use computer systems, facilities or services in any way that diminishes or interferes with the reasonable and confidential use of those systems.

The College retains the right to access and immediately remove any data or files evidencing any such misuse.

Account access information assigned to an individual is not to be given to another individual. The individual assigned to an account is responsible for all activity for which that account is used.

The following policies govern the use of all college computing facilities. Any use of these facilities in any way other than those stated below will be considered in violation of college policy.

* Users are accountable for using computing facilities in an effective, ethical and lawful manner.

* 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 college-related functions.

* Illegal material may not be accessed, viewed or stored on college computing facilities.

* 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.

Software Use Policies:

Neither licensed software, nor college-developed software, shall be copied except as specifically stipulated in license agreements or in The Texas State University System Rules and Regulations. All software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright.

Students have permission to use licensed software according to the regulations set by the College. The use of such software is governed by the terms of licensing agreements between the College and the software licensors. Users must read and abide by the terms of those agreements.

Software applications shall not be used to create, modify, access, view, display or activate files, information or materials that are offensive, indecent or illegal.

Manuals, and other copyrighted materials, shall not be copied without specific, written permission of the publisher.

Internet Use Policies:

The College maintains a connection to the internet in support of its mission. Users must be aware that all internet usage, including source and destination, can be recorded and stored. Users have no right to privacy with regard to internet use.

The College has the ability and right to view any user's usage patterns and take action to assure internet resources are devoted to maintaining the highest levels of productivity.

The internet path record is the property of the College and therefore the people of the State of Texas. Such information is subject to the Texas Public Information Act and the state laws applicable to records retention.

Using the college's internet connection to access information, images or other materials that violate any federal laws, state laws, Texas State University System rules or LSC-PA policies is strictly prohibited. Using the internet connection to access other computer systems in violation of state or federal law is prohibited. Using the internet connection to access other computer systems in violation of the policies of the entity that owns those systems is strictly prohibited.

Electronic Messaging Policies:

Access to and the responsible use of modern information resources are essential to the pursuit and achievement of excellence. The College encourages the appropriate use of electronic messaging to enhance productivity. Use of these resources must be consistent with the college's goals of education, research, and public service.

"Electronic messaging" refers to those computer applications such as email, instant messaging, video and/or audio conferencing/collaboration, chat rooms, newsgroups, list servers, streaming media, message boards or any other application that allows a user to interactively or passively communicate with one or more persons or entities using the college computing or communications resources.

Responsible users of electronic messaging applications are expected to act in accordance with the following policies based on common sense, common decency and civility applied to the networked computing environment.

Information sent as electronic messages should meet the same standards for distribution or display as if they were tangible documents or instruments. Users must be clearly and accurately identified in all electronic communications.

Concealing or misrepresenting a name or affiliation in order to be dissociated from responsibility for actions taken is never appropriate. Alteration of the source of

electronic messages or postings is unethical and possibly illegal.

Electronic messaging facilities are for college-related activities only. All electronic messaging files belong to someone. Aside from the college's right of access, they should be assumed to be private and confidential unless the owner has explicitly made them available to others.

The College cannot guarantee the privacy or confidentiality of electronic documents or communications.

Users must respect the rights of others and must not send, post or broadcast abusive, threatening, illegal, indecent or harassing materials. While debate on controversial issues is inevitable and essential, users must do so in a way that actually advances the cause of learning and mutual understanding.

Electronic messaging and other network resources may not be used for commercial purposes or for personal financial gain.

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.

Telephone System Use Policies:

Lamar State College-Port Arthur telephone facilities are intended to support the academic mission and the administrative functions of the College. The policy states the principles regarding the use of the telephone system.

The college's telephone facilities include any telephone or voice communication device including the Phone Mail System.

Users shall:

* Be accountable for using these facilities in an effective ethical and lawful manner.

* Only use those facilities for which they have authorization, whether these facilities are at the College or at any other facility accessible through the telephone network.

* Take all reasonable steps to protect the privacy of others as well as the integrity of the College. Users shall not share with others PIN numbers, passwords, or any other authorization which has been assigned to them.

* Be aware that all calls are monitored by a Call Detail Recording System located in the Computer Center. These reports are published to the President, Vice President of Academic Affairs and the Director of Computer Services monthly and are available to the Department Chairs upon written request.

Consequences of Information Resources Policy Violations

An individual's computing and communications resources use privileges may be suspended or restricted immediately upon discovery of any policy violation. Removal of the suspension or restriction will be by appeal to the Director of Information Technology Services or the Vice President for Academic Affairs. Continued or major violations of these policies may result in the College exercising its right to deny future computing privileges. In addition, any user found in violation may also be subject to further disciplinary action by the College, including termination of employment or suspension from school, 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.

Disciplinary Action

Students are subject to disciplinary action for unacceptable behavior, as outlined in the Student Handbook under "Student Conduct and Discipline." The Vice President for Student Services may classify behavior as unacceptable and may refer the case to the proper judicial body for investigation and decision. The student has the privilege of appealing the decision to the College Discipline Committee. This appeal is made through the Office of the Vice President for Student Services and the action of the College Discipline Committee is subject to review by the President.

Health Insurance

All full-time students are eligible to purchase health and accident insurance. A brochure explaining the coverage, cost and benefits is available in the offices of the Vice President for Student Services and the Director of Student Activities.

Proof of health and accident insurance is required of all foreign students and all participants in intramural/recreational or intercollegiate sports programs.

Information Resources Policy

I. Overview

A.Purpose and Scope

The purpose of this Policy is to define Information Resource Operating Policies for the management and security of Lamar State College-Port Arthur information resources.

B.Authority

The contents of the Policies listed below ensure the college's compliance with *Texas Administrative Code (TAC) 202* and the *Texas State University System Rules and Regulations*.

II. Security Violations and Sanctions

Information resources are valuable assets strategically provided to further the instructional, research, 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 all College policies, procedures, as well as 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.

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. Any actual or suspected security violation should be reported immediately to the Director of Information Technology Services at 409-984-6484 or to the Assistant Director of Systems, Networking, and Telecom at 409-984-6141.

B. 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 College 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.

III. Information Resources Policies
Responsibilities – Authority – TAC 202.70; 202.71; 202.72; 202.75

1. The IRM shall produce annually for review and approval by the president of the College a document identifying College information resource ownership and associated responsibilities for all information resource assets. (TAC 202.71.a)
2. The IRM shall produce annually for review and approval by College information resource owners a document identifying information resource custodians and approved users. (TAC 202.71.c)
3. The president of the College shall appoint an Information Security Officer (ISO) who shall report to executive management of the College. (TAC 202.71.d)
4. The Information Security Officer shall document and maintain an up-to-date information security program. At a minimum the security program will be defined as the aggregate of policies compliant with TSUS rules and regulations Chapter III Paragraph 19 and TAC Chapter 202, Subchapter C, Rule 202.70 through Rule 202.78. The information security program shall be approved by the president of the College. (TAC 202.70.2, 202.71.d.2)
5. The Information Security Officer shall report annually to the president of the College the status and effectiveness of information resource security controls. (TAC 202.71.d.4, 202.72.c)
6. The Information Security Officer, in cooperation with information owners and custodians, shall develop and recommend policies, procedures, and practices necessary to ensure the security of information resources against unauthorized or accidental modification, destruction, or disclosure. (TAC 202.71.d.1&5)
7. The IRM and Information Security Officer shall establish a network perimeter protection strategy which includes some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router. (TAC 202.75.8)
8. The IRM shall ensure that an independent, third party, biennial review of the information security program is performed. (TAC 202.71.e)

5.16.2 Data Classification and Risk Assessment – Authority-TAC 202.70; 202.71; 202.72; 202.74; 202.76

All data owners or designated custodians shall be responsible for classifying data processed by systems under their purview based on data sensitivity so that the appropriate security controls can be applied and the information resource can be appropriately managed. (TAC 202.71.c.1.I)

The Data Classification document produced annually by the ISO shall be used to identify data types and their need for confidentiality, integrity, and availability. (TAC 202.71.b, 202.76.a.3)

A data classification of Category-I shall be based on compliance with applicable federal or state law, a contract, or on the demonstrated need to: (TAC 202.71.b, 202.76.a.3)

- Document the integrity of that digital data (that is, confirm that data was not altered intentionally or accidentally),
- Restrict and document individuals with access to that digital data, and
- Ensure appropriate backup and retention of that digital data.

Certain digital data not defined as Category-I digital data can be so classified if warranted by a department's demonstrated need. With suitable justification, the college may convert its classification of these digital data from Category-I digital data to a lesser classification upon request by the data owner, with IRM review and approval. (TAC 202.71.c.1.I, 202.72.c)

Under the guidance of the Information Security Officer, the college shall annually conduct and document an information security risk assessment. (TAC 202.72.a, 202.73.b, 202.74.a.2)

The confidentiality, integrity, and availability of information resources shall be managed and protected based on sensitivity and risk. (TAC 202.70.1)

The IRM produce and maintain a procedure manual consisting of IRM reviewed and approved procedures for the management and operation of information resource assets.

5.16.1 Physical and Environmental Security Policy – Authority-TAC 202.73; 202.75

1. All physical security and environmental control systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
2. All information resource facilities must be protected against loss from both physical and environmental threats in proportion to the

category of data or systems housed within the facility. (TAC 202.73.a)

3. Physical access to all restricted information resource facilities must be documented and managed. (TAC 202.73.a)
4. The process for granting card and/or key access to information resource facilities must include the approval of the person responsible for the facility. (TAC 202.75.7.P)
5. Requests for access must be approved by the department head and authorized by the IRM. (TAC 202.75.7.P)
6. Card and/or key access to information resource facilities must be granted only to college support personnel, and contractors, whose job responsibilities require routine access to that facility. (TAC 202.75.7.P)
7. Each individual that is granted access rights to an information resource facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements. (TAC 202.75.7.P)
8. Access cards, codes, and/or keys must be changed on a periodic basis based on the criticality or importance of the facility. (TAC 202.75.7.P)
9. Access cards, codes, and/or keys must not be shared, reallocated, or loaned to others.
10. Access cards and/or keys that are no longer required must be returned to the person responsible for the information resource facility. (TAC 202.75.7.P)
11. Lost, stolen, or compromised access cards, codes, and/or keys must be reported to the person responsible for the information resource facility. (TAC 202.75.7.P)
12. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned. (TAC 202.75.7.P)
13. Cards and/or keys must not have identifying information other than a return mail address. (TAC 202.75.7.P)
14. All information resource facilities that allow access to visitors will track visitor access with a sign in/out log. (TAC 202.75.7.P)
15. Visitors must be escorted in authorized access controlled areas of information resource facilities. (TAC 202.75.7.P)
16. Access records and visitor logs must be kept for review. (TAC 202.75.7.P)
17. The card and/or key access rights of individuals that change roles within the college or are separated from their relationship with the college shall be removed. (TAC 202.75.7.P)
18. Access records and visitor logs for an information resource facility shall be reviewed on a periodic basis and any unusual access investigated. (TAC 202.75.7.P)
19. Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed. (TAC 202.75.7.P)

5.16.2 Backup and Business Continuity – Authority-TAC 202.70; 202.74; 202.75

1. The IRM is responsible for developing and maintaining a Disaster Recovery Plan designed to address the operational restoration of the college's critical computer processing capability. The plan will integrate into and meet the objectives of the larger Business Continuity Plan for the college and be reviewed on the same schedule. (TAC 202.70.6, 202.74.a)
2. 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. (TAC 202.74.b)
3. The vendor(s) providing offsite backup storage, if any, for the college must be cleared to handle the highest level of information stored. (TAC 202.75.7.E)
4. 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 college's highest sensitivity level of information stored. (TAC 202.75.7.E)
5. The backup and recovery process for each system must be documented and periodically reviewed. (TAC 202.75.7.E)
6. A process must be implemented to verify the success of the college electronic information backup. (TAC 202.75.7.E)
7. Backups must be periodically tested to ensure that they are recoverable. (TAC 202.75.7.E)
8. Procedures between the college and the offsite backup storage vendor(s), if any, must be reviewed and approved periodically by the IRM. (TAC 202.75.7.E)

5.16.5 Portable Computing and Encryption – Authority-TAC 202.75

1. Only portable computing devices approved by the IRM may be used to access college information resources. (TAC 202.75.7.Q)
2. College owned portable computing devices must be password protected. (TAC 202.75.7.Q)
3. College data should not be stored on portable computing devices or portable storage devices/media. Specific, written permission shall be obtained from the data owner before a user may store Category-I college data on a portable computing or storage device/media. (TAC 202.75.7.Q)
4. Category-I/II college data shall not be copied to or stored on portable computing devices, portable storage device/media or non-college owned portable computing device in a non-encrypted state. (TAC 202.75.4, 202.75.7.H)
5. Category-I/II college data must not be transmitted on a public network or via wireless network unless approved encryption techniques and/or approved wireless transmission protocols are utilized. (TAC 202.75.4, 202.75.7.H, 202.75.7.Z.ii)

6. The ISO is responsible for determining the approved encryption methods for storing and transmitting college data. (TAC 202.75.4, 202.75.7.H, 202.75.7.Z.ii)
7. 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 locked in a secure, out-of-sight area of a vehicle. (TAC 202.75.7.Q)

5.16.6 System Development and Auditing – Authority- TAC 202.71; 202.75

1. The Information Technology Services Department is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for college 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; security implications; 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 college information. (TAC 202.75.6.B, 202.75.7.D, 202.75.7.U, 202.75.7.W)
2. All production systems must have designated owners and custodians. (TAC 202.71.c)
3. All production systems must have an access control system suited to the classification of data stored on the system as determined by the risk analysis process. (TAC 202.75.3.C)
4. Where resources permit, there shall be a separation between the production, development, and test environments. All development and testing environments must utilize sanitized data or maintain the same security access as the production system. (TAC 202.75.6.A)
5. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production. (TAC 202.75.7.D)
6. Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of Category-I data. (TAC 202.75.5.A)
7. Appropriate audit trails shall be maintained to provide accountability for updates to Category-I data and related hardware and software, and for all changes to automated security or access rules. (TAC 202.75.5.B)
8. Based on the risk assessment completed by the ISO, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system. (TAC 202.75.5.C)
9. Where possible a logon banner/warning should be presented when a user logs on to a system. The ISO shall approve the content of the banner/warning. (TAC 202.75.9)

5.16.7 Acceptable Use – Authority – TAC 202.70; 202.75

1. Lamar State College – Port Arthur information resources are finite by nature. All users must recognize that certain uses of college owned information technology resources may be limited or regulated as required to fulfill the college's primary teaching, research and public service missions.
2. Users must report any weaknesses in computer security, any incidents of possible misuse or violation of this agreement to the Information Security Officer. (TAC 202.75.7.A)
3. Users must not attempt to access any data or programs contained on college systems for which they do not have authorization or explicit consent to do so. (TAC 202.75.7.A)
4. Users must not share their college account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. (TAC 202.75.7.A)
6. Users are responsible for all actions that take place with their account. (TAC 202.70.3)
7. Users must distinguish between ideas, comments, and opinions of the individual user versus those that represent the official positions, programs, and activities of the college.
8. The college is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet or world wide web, that reflect only the personal ideas, comments and opinions of individual members of the college community, even where they are published or otherwise circulated to the public at large by means of college information technology resources.
9. Students, faculty and staff using information technology resources for purposes of exchanging, publishing or circulating official institutional documents must follow LSC-PA requirements concerning appropriate content, style and use of logos, seals, or other official insignia.
10. Users of college information resources must not use any software not provided by the college without Information Technology Services Department approval. (TAC 202.75.7.V)
11. Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of college information resources; deprive an authorized Lamar State College - Port Arthur user access to a college resource; obtain extra resources beyond those

allocated; circumvent any computer security measures. (TAC 202.75.7.A)

12. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on college information resources. (TAC 202.75.7.V)
13. Lamar State College - Port Arthur information resources must not be used for personal benefit, political lobbying or campaigning. (TAC 202.75.7.A)
14. Users must not intentionally create, access, store, view or transmit material which the college 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 college's official processes for dealing with academic ethical issues). (TAC 202.75.7.L)
15. Illegal material may not be used to perform any legitimate job or academic function and therefore may not be created, accessed, stored, viewed, or transmitted on college information resources. (TAC 202.75.7.L)
16. 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 access to college computer systems. (TAC 202.75.7.A)
17. 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. (TAC 202.75.7.A)
18. All user activity on college information resources assets is subject to logging, monitoring, and review. (TAC 202.75.7.A)
19. Privately owned information resources are subject to the Acceptable Use Policy when used or operated on campus. (TAC 202.75.7.A)
20. As a convenience to the Lamar State College - Port Arthur user community, some incidental use of information resources is permitted. The following restrictions apply: (TAC 202.75.7.A, 202.75.7.G, 202.75.7.L)
    a. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, telephones, and so on, is restricted to college approved users; it does not extend to family members or other acquaintances.
    b. Incidental use must not result in direct costs to the college.
    c. Incidental use must not interfere with the normal performance of an employee's work duties.
    d. No files or documents may be sent or received that may cause legal action against, or embarrassment to, the college.
    e. Storage of personal email messages, voice messages, files and documents within the college's information resources must be nominal.
    f. All messages, files and documents – including personal messages, files and documents – located on college information resources are owned by the college, may be subject to open records requests, and may be accessed in accordance with this policy.
    g. Non-business related purchases made over the internet are prohibited.

5.16.8 Account Management – Authority-TAC 202.71; 202.75; 202.77

1. All access requests for Category I/-II information resources shall follow an account creation process that includes appropriate approvals. (TAC 202.75.1, 202.75.2.A)
2. Users must sign the appropriate Lamar State College - Port Arthur Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to a Category-I/II information resources. (TAC 202.77.a, 202.77.c)
3. All accounts must be uniquely identifiable using a centrally assigned user name from the Information Technology Services Department. (TAC 202.75.3.A)
4. All accounts have a password construction and expiration that complies with the college Password Security Guidelines issued by the ISO. (TAC 202.75.3.D, 202.75.7.K)
5. Accounts of individuals, who have had their status, roles, or affiliations with the college change or who have become separated from the university, shall be updated or revoked to reflect their current status. (TAC 202.75.3.B)
6. Accounts of individuals on extended leave (more than 90 days) may be disabled at the discretion of the IRM. (TAC 202.75.3.B)
7. Accounts should be reviewed periodically by system administrators and data owners to ensure their status is correct. (TAC 202.71.c.1.G)
8. All vendor, consultant, and contractor accounts shall follow this policy. (TAC 202.75.2.B, 202.75.7.X, 202.77.c)

5.16.9 Administrator/Special Access – Authority-TAC 202.75

1. All users of system administrator or other special access accounts must be authorized by the IRM, ISO, and data owners. (TAC 202.75.7.C)
2. Users must sign the appropriate Lamar State College - Port Arthur Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an administrator or other special access account. (TAC 202.75.7.C)

3. All users of system administrator or other special access accounts must have account management instructions, documentation, training, and follow guidelines developed by the ISO. (TAC 202.75.7.C)
4. The password for a shared administrator/special access account must change when an individual with the password leaves the department or college, or upon a change in the third party vendor personnel assigned to a college contract. (TAC 202.75.7.C)
5. When special access accounts are needed for internal or external Audit, software development, software installation, or other defined need, they: (TAC 202.75.7.C)
    - ❖ must be authorized by the system or data owner
    - ❖ must be created with a specific expiration date
    - ❖ must be removed when work is complete

5.16.10 Change Management Policy – Authority-TAC 202.70; 202.75

1. Every change to a college 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 in the Information Technology Operations Manual. (TAC 202.70.5, 202.75.7.F)
2. A Change Management Committee for system containing or managing Category-I data, appointed by the IRM, will meet regularly to review change requests, and to ensure that change reviews and communications are being satisfactorily performed. (TAC 202.70.5, 202.75.7.F)
3. Changes to systems containing or managing Category-I data must be well documented and receive written approval from the data owners for that system prior to implementation. (TAC 202.70.5, 202.75.6.C)

5.16.11 Incident Management – Authority-TAC 202.75; 202.76

1. Whenever a security incident is suspected or confirmed, the appropriate incident management procedures as defined by the ISO must be followed. (TAC 202.75.7.J)
2. All unauthorized or inappropriate disclosures of Category-I data shall be reported promptly to the Information Security Officer. (TAC 202.76.a)
3. The college shall disclose, in accordance with applicable federal or state law, incidents involving computer security that compromise the security, confidentiality, and/or integrity of personally identifying information it maintains to data owners and any resident of Texas whose personally identifying information was, or is reasonably believed to have been, acquired without authorization. (TAC 202.76.a.3)
4. The ISO is responsible for reporting the incident to the:
    - ❖ Department of Information Resources as outlined in TAC 202.(TAC 202.76.a)
    - ❖ Local, state or federal law officials as required by applicable statutes and/or regulations (TAC 202.76.b)
5. The ISO is responsible for coordinating communications with outside organizations and law enforcement and act as the liaison between law enforcement and the college. (TAC 202.76.a, 202.76.c)
6. The ISO shall make monthly summary incident reports to the Department of Information Resources in the manner the department determines. (TAC 202.76.d)

5.16.12 Password Security Policy – Authority-TAC 202.75

1. All passwords, including initial passwords, must be constructed and implemented according to the Information Technology Services Department requirements for password characteristics such as length, complexity, age, and reuse. (TAC 202.75.7.K)
2. Stored passwords must be encrypted. (TAC 202.75.7K)
3. User account passwords must not be divulged to anyone. (TAC 202.75.7.K)
4. Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the college. (TAC 202.75.7.K)
5. If the security of a password is in doubt, the password must be changed immediately. (TAC 202.75.7.K)
6. Administrators must not circumvent the Password Security Policy for the sake of ease of use. (TAC 202.75.7.K)
7. Users must not 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 college ISO. In order for an exception to be approved there must be a procedure to change the passwords. (TAC 202.75.7.K)
8. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device. (TAC 202.75.7.K)
9. Information Technology Services Department Helpdesk password change procedures must include the following: (TAC 202.75.7.K)
    - ❖ verify the identity of the user before changing password
    - ❖ change to a password that meets Information Technology Services Department guidelines for password characteristics.

5.16.13 Intrusion Detection – Authority-TAC 202.75

1. The ISO will develop a schedule for frequent, routine reviews of log files of systems containing Category-I data as identified through risk assessments. (TAC 202.75.7.M)
2. The ISO will develop a schedule for frequent, routine review of log files of any firewalls, Intrusion Detection, and other network perimeter devices. (TAC 202.75.7.M)
3. The ISO will develop a schedule for routine system integrity checks of the firewalls and other network perimeter access control systems. (TAC 202.75.7.M, 202.75.7.AA)
4. All trouble reports should be reviewed for symptoms that might indicate intrusive activity. (TAC 202.75.7.M)
5. All suspected and/or confirmed instances of successful intrusions must be immediately reported according to the Incident Management Policy. (TAC 202.75.7.M)
6. Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the ISO. (TAC 202.75.7.M)

5.16.14 Network Access – Authority-TAC: 202.75; 202.77

1. Use of the college network constitutes acknowledgement of and agreement to abide by all policies set forth in the Acceptable Use Policy. (TAC 202.77.a, 202.77.b)
2. Use of the college network must be consistent with and in support of college initiatives.
3. Users are permitted to use only those network addresses issued to them by the Information Technology Services Department. (TAC 202.75.7.N)
4. All remote access to the college internal network must be authorized by Information Technology Services Department. (TAC 202.75.7.N)
5. Authorized remote users may connect to college information resources only through an approved ISP and using protocols approved by the college. (TAC 202.7.7.N)
6. Users may not be simultaneously connected to the college internal network and any external network. (TAC 202.75.7.N)
7. Users must not extend or re-transmit network services in any way. (TAC 202.75.7.N)
8. Users must not install or alter network hardware or software in any way. (TAC 202.75.7.N)
9. Non college owned computer systems that require network connectivity must conform to LSCPA Information Technology Services Department requirements.
10. Network devices that pose an immediate threat to network operations, performance, or other network-connected devices must be disconnected or quarantined to minimize risk until the threat is removed (TAC 202.75.7.N)

5.16.15 Network Management and Configuration – Authority- TAC 202.75

1. The Information Technology Services Department owns and is solely responsible for the management or administration of the college data and telephony network infrastructure including, but not limited to, the following: (TAC 202.75.7.O)
    - Installation, configuration and operation of all switches, routers, wireless devices, and firewalls (TAC 202.75.7.I, 202.75.7.Z.i)
    - Installation, configuration and operation of active network management devices
    - Establishment and management of all protocols used on the college network (TAC 202.75.7.I)
    - Network address allocation and distribution
    - All connections to external third party data and telephony networks
    - All communications cabling installation or modification
    - Extension or re-transmission of network services in any way
    - Configuration and broadcast of all wireless signals providing access to the college network (TAC 202.75.7.Z.i, 202.75.7.Z.iii)
    - Installation and configuration of all telephony devices
    - Creation and maintenance of all college network infrastructure standards and guidelines (TAC 202.75.7.I)
    - Creation and maintenance of a directory of network devices

    1. Any device connected to the college network is subject to Information Technology Services Department management and monitoring standards. (TAC 202.75.7.O)

5.16.16 Information Resources Privacy Policy – Authority-TAC 202.75

1. Electronic files and data created, sent, received, stored, or transmitted across computers or other information resources owned, leased, administered, or otherwise under the custody and control of the college are not private unless expressly stated in federal or state law and may be accessed at any time by the college administration, following a defined approval process, without knowledge of the information resource user or owner. Applicable open records requests shall follow the college standard formal request process. (TAC 202.75.7.R)
2. The college may log, review, capture, and otherwise utilize information stored on or passing through its information resources as needed for the purpose of system administration and maintenance, for

resolution of technical problems, for compliance with Texas Public Information Act, for compliance with federal or state subpoenas, court orders, or other written authorities, allow institutional officials to fulfill their responsibilities when acting in their assigned capacity, and to perform audits. No notification is required to view this information; however, users with privileged access are expected to maintain the privacy of the individual. (TAC 202.75.7.R)

3. Identifying information shall be removed before sharing collected information to prevent loss of individual privacy where possible. (TAC 202.75.7.R)
4. Employees, contractors, vendors, and affiliates of the college shall safeguard the privacy and security of any information owned by or entrusted to the college. (TAC 202.75.7.R)
5. Disclosure of personally identifiable information to unauthorized persons or entities is expressly forbidden. (TAC 202.75.7.R)
6. Efforts shall be made to reduce the collection and use of personally identifiable information. If the information is required to be collected by state or federal law, the individuals shall be informed of the requirement on the form or at the time of collection. (TAC 202.75.7.R)
7. Access to personally identifiable information shall be granted through an appropriate approval process and be revalidated on a regular basis. (TAC 202.75.7.R)
8. Paper and electronic documents containing personally identifiable information shall be secured during use and when not in use. (TAC 202.75.7.R)
9. Electronic documents containing personally identifiable information shall only be stored on authorized systems. (TAC 202.75.7.R)

5.16.17 Security Monitoring – Authority-TAC 202.71; 202.75

1. To ensure compliance with these policies, state laws and regulations related to the use and security of information resources, the college's Information Security Officer has the authority and responsibility to monitor information resources to confirm that security practices and controls are adhered to and are effective. (TAC 202.71.d.3)
2. Routine monitoring and analysis of operating system, application, and network device logs are required on a schedule consistent with the ISO risk assessment. (TAC 202.75.7.S)
3. Backup strategies for security logs should be consistent with the ISO risk assessment. (TAC 202.75.7.S)
4. Logging of all administrator and root access should be consistent with the ISO risk assessment. (TAC 202.75.7.S)
5. Any security issues discovered will be reported to the ISO for follow-up investigation. (TAC 202.75.7.S)

5.16.18 Security Awareness and Training – Authority-TAC 202.75; 202.77

1. All new users must attend an approved Security Awareness training session prior to, or at least within 30 days of, being granted access to any college information resources. (TAC 202.75.7.T, 202.77.e)
2. All users must sign an acknowledgement stating they agree to the college's requirements regarding computer security policies and procedures. (TAC 202.75.7.T)
3. Information Technology Services shall deliver security awareness training on a periodic basis. (TAC 202.75.7.T, 202.77.d)
4. All employees must participate in a periodic computer security awareness presentation. (TAC 202.75.7.T, 202.77.d)

5.16.19 Server Management and Hardening – Authority-TAC 202.75

1. The IRM will create and maintain a server registration that will include the designated server owner and server administrator(s) and other information necessary to indicate the purpose and function of the server supports and is consistent with college initiatives.
2. A server owner shall be designated by the IRM for each server. The server owner shall be responsible for establishing server usage policies, specifying server access controls (both physical and electronic), and assuring compliance with state and college server management standards. Data owners may be server owners.
3. A server administrator shall be designated by the server owner for each server. The server administrator shall be responsible for enforcing the owner's usage policies, implementing the owner-specified access controls, and configuring the server according to the required standards. Data custodians may be server administrators.
4. The IRM shall produce and maintain a server management guide that includes server management standards and best practices for college owned servers. All servers must be maintained to the standard set forth in the guide unless an exception has been made based on a documented risk management decision.
5. A server must not be connected to the college network until it is in an Information Technology Services Department accredited secure state and the network connection is approved by Information Technology Services Department. (TAC 202.75.7.U)
6. The degree of hardening for operating systems and applications shall be in accordance with the importance of the information on the system and the acceptable risk as determined by the data owner. (TAC 202.75.7.U)
7. Information Technology Services Department will monitor security issues, both internal to the college and externally, and will manage the

release of security patches on behalf of the college. (TAC 202.75.7.U)

8. Information Technology Services Department may make hardware resources available for testing security patches in the case of special applications. (TAC 202.75.7.U)
9. Security patches must be implemented within the specified timeframe of notification from the Information Technology Services Department. (TAC 202.75.7.U)
10. Servers that pose an immediate threat to network operations, performance, or other network-connected devices must be disconnected or quarantined to minimize risk until the threat is removed.

5.16.20 Software Licensing – Authority-TAC 202.75

1. Copies of software licensed by the college shall not be made without verifying that a copy is permitted via the license agreement. (TAC 202.75.7.V)
2. Software used on college-owned systems shall be properly licensed for their method of use (concurrent licensing, site licensing, or per system licensing). (TAC 202.75.7.V)
3. The college has the right to remove inappropriately licensed software from college computers if the user is not able to show proof of license. (TAC 202.75.7.V)
4. Software license management shall be achieved through central purchasing oversight.

5.16.21 Computer Related Purchasing and Support – Authority-TAC 202.70; 202.75

1. The IRM must approve all information technology related software and hardware purchases regardless of source of funds, including any device capable of storing, transmitting or processing electronic college owned data. This applies to information resources acquired as part of a larger or non-IT purchase or contract. (TAC 202.70.7, 202.75.7.W)
2. The Information Technology Services Department will conduct all quotes for bids and prices.
3. Each division, department, and office should consult with the Information Technology Services Department when preparing its annual budget for assistance in developing its requests for funds for hardware and software acquisitions. (TAC 202.75.7.W)
4. All college owned information resources, hardware and software, will be managed, facilitated, or provided by the Information Technology Services department.

5.16.22 Vendor Access – Authority-TAC 202.75

1. Vendors must comply with all applicable college policies, practice standards and agreements. (TAC 202.75.2.B, 202.75.7.X)
2. Vendor agreements and contracts must specify: (TAC 202.75.2.B, 202.75.7.X)
   - The college information resources to which the vendor should have access
   - How the college information is to be protected by the vendor
   - Acceptable methods for the return, destruction or disposal of the college's information in the vendor's possession at the end of the contract
   - The vendor must only use the college's data and information resources for the purpose of the business agreement
   - Any other college data acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
   - Upon termination of contract or at the request of college, the vendor will return or destroy all college data and provide written certification of that return or destruction within 24 hours.
3. Each vendor employee with access to college data must be approved by the data owner to handle data of that classification. (TAC 202.75.2.B, 202.75.7.X)
4. Vendor personnel must report all security incidents directly to the appropriate Lamar State College - Port Arthur personnel. (TAC 202.75.2.B, 202.75.7.X)
5. If the vendor is involved in college security incident management the responsibilities of the vendor must be specified in the contract. (TAC 202.75.2.B, 202.75.7.X)
6. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate college personnel. (TAC 202.75.2.B, 202.75.7.X)
7. Vendors are required to comply with all federal, state and Lamar State College - Port Arthur auditing requirements, including the auditing of the vendor's work. (TAC 202.75.2.B, 202.75.7.X)

5.16.23 Malicious Code – Authority-TAC 202.75

1. All workstations and servers, whether connected to the college network, or standalone, must use the Information Technology Services Department approved virus and malware protection software and configuration. (TAC 202.75.7.Y)
2. The virus and malware protection software must not be disabled or bypassed. (TAC 202.75.7.Y)
3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software. (TAC 202.75.7.Y)
4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates. (TAC 202.75.7.Y)

5. Any system identified as a security risk due to a lack of anti-malware software may be disconnected from the network, or the respective network account may be disabled, until adequate protection is in place. (TAC 202.75.7.Y)
6. Every virus that is not automatically cleaned or quarantined by the virus protection software must be reported to the Information Technology Services Department Help Desk. (TAC 202.75.7.Y)

5.16.24 Data Disposal and Destruction – Authority-TAC 202.78

1. Prior to the sale, transfer, or other disposal of information resources, the Information Technology Services Department will assess whether to remove data from any associated storage device. (TAC 202.78.b.1)
2. Electronic state records shall be destroyed in accordance with §441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, the college shall retain a hard copy or other electronic copy of the record for the required retention period. (TAC 202.78.b.2)
3. If it is possible that Category-I/II information resources are contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. (TAC 202.78.b.3)
4. The college shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information: (TAC 202.78.b.4)
    - ❖ date
    - ❖ description of the item(s) and serial number(s)
    - ❖ inventory number(s)
    - ❖ the process and sanitization tools used to remove the data or method of destruction
    - ❖ the name and address of the organization the equipment was transferred to.

5.16.25 Peer-to-Peer (P2P) – Authority-TAC 202.75; *Executive Order (RP58)*

1. 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 IRM. (TAC 202.75.7.V)
2. Any permitted use of P2P software is subject to all information resource policies including the Acceptable Use policy. (TAC 202.75.7.V)

Official Summons

An official summons takes precedence over other college activities of the student and should be answered promptly on the day and hour designated. Failure to heed an official summons may subject the student to serious disciplinary action.

Personal Information

Personal information, such as an address and telephone number, is used to communicate with students. Students are responsible for notifying Lamar State College Port Arthur of any change of name, address, and/or telephone number. Changes must be reported to Student Services. Students may request that directory information not be shared. To prevent the sharing of directory information, students must complete a Release of Information Form and deliver it to the Records Office. The Release of Information Form may be obtained at the Student Services office.

Change of name due to marriage or correction of name because of spelling errors may be made by completing a name change card. All name changes must be accompanied by a copy of the legal document making the name change official. This document will be kept on file in the student's confidential folder. Former student names will be displayed on all official transcripts.

Family Education Rights and Privacy Act of 1974

The following information concerning student records maintained by LIT is published in compliance with the Family Education Rights and Privacy Act of 1974 (PL 93-380).

Access to educational records directly related to a student will not be granted unless disclosure of the type of record is authorized to be disclosed under the provision of the law. The types, locations, and names of custodians of educational records maintained by LSCPA are available from the Registrar. Access to records by persons other than the student will be limited to those persons and agencies specified in the statute.

The release of information to the public without the consent of the student will be limited to the categories of information which have been designated by Lamar State College Port Arthuras directory information and which will be routinely released. The student may request that any or all of this information be withheld from the public by making written request to the Student Services Office. Forms for submitting the written request to withhold director information are available in the Office of Student Services. The request must be made by the last official day to register for a given session and applies until a written release is received. Directory information includes name, current and permanent address, E-mail, telephone listing, date and place of birth, major and minor, semester hour load, classification, participation

in officially recognized activities, dates of attendance, degrees and awards received with dates, and the last educational agency or institution attended.

One exception which permits disclosure without consent is disclosure to school officials with legitimate educational interests. A school official is a person employed by Lamar State College Port Arthur or the Texas State University System Administrative Office in an administrative, supervisory, academic research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the LSCPA has contracted (such as an attorney, auditor or collection agent); a person serving on the Board of Regents; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

A school official has a legitimate educational interest if the official needs to review an educational record in order to fulfill his or her professional responsibility.

Upon request, the LSCPA discloses education records without consent to officials of another school, in which a student seeks or intends to enroll.

A student has the right to challenge records and information directly related to him or her if it is considered to be inaccurate, misleading or otherwise inappropriate. Issues may be resolved either through an informal hearing with the official immediately responsible or by requesting a formal hearing. The procedures to be followed in a formal hearing are available in the Office of Student Services. The right of parental access to student records may be established by either of two methods: first, by the student's filing a written consent statement, or second, by the parent validating the student's dependency as defined by the Internal Revenue Service.

Bacterial Meningitis

Information about bacterial meningitis is being provided to new college students in the State of Texas. Bacterial Meningitis is a serious, potentially deadly disease that can progress extremely fast, so take utmost caution. It is an inflammation of the membranes that surround the brain and spinal cord. The bacteria that causes meningitis can also infect the blood. This disease strikes about 3,000 Americans each year, including 100-125 on college campuses, leading to 5-15 deaths among college students every year. There is a treatment, but those who survive may develop severe health problems or disabilities.

What are the symptoms?

- High fever.
- Severe headache.
- Rash.
- Vomiting.
- Rashes on skin.
- Stiff neck.
- Light sensitivity.
- Nausea.
- Confusion
- Seizures.
- Lethargy.

There may be a rash of tiny, red-purple spots caused by bleeding under the skin. These can occur anywhere on the body. The more symptoms, the higher the risk, so when these symptoms appear seek immediate medical attention.

How is bacterial meningitis diagnosed?

- Diagnosis is made by a medical provider and is usually based on a combination of clinical symptoms and laboratory results from spinal fluid and blood tests.
- Early diagnosis and treatment can greatly improve the likelihood of recovery.

How is the disease transmitted?

The disease is transmitted when people exchange saliva (such as by kissing, or by sharing drinking containers, utensils, cigarettes, toothbrushes, etc.) or come in contact with respiratory or throat secretions.

How do you increase your risk of getting bacterial meningitis?

- Exposure to saliva by sharing cigarettes, water bottles, eating utensils, food, kissing, etc.
- Living in close conditions (such as sharing a room/suite in a dorm or group home).

What are the possible consequences of the disease?

- Death (in 8 to 24 hours from perfectly well to dead).
- Permanent brain damage.
- Kidney failure.
- Learning disability.
- Hearing loss, blindness.
- Limb damage (fingers, toes, arms, legs) that require amputation.
- Gangrene.
- Coma.
- Convulsions.

Can the disease be treated?

- Antibiotic treatment, if received early, can save lives and chances of recovery are increased. However, permanent disability or death can still occur.

Vaccinations are available and should be considered for:

- Those living in close quarters.
- College students 25 years old or younger.

- Vaccinations are effective against four of the five most common bacterial types that cause 70 percent of the disease in the U.S. (but do not protect against all types of meningitis).
- Vaccinations take 7-10 days to become effective, with protection lasting 3 to 5 years.
- The cost of vaccine varies, so check with your health care provider.
- Vaccination is very safe. Most common side effects are redness and minor pain at injection site for up to two days.
- Vaccination is available at the Student Health Center.

How can I find out more information?

- Contact your own health care provider.
- Contact your Student Health Center at (409) 880-8466.
- Contact your local or regional Texas Department of Health office at (409) 832-4000.
- Contact Web sites: www.cdc.gov; *www.acha.org/*.

Drug-Free Workplace Policy

1. Purpose

1.1 Based on its commitment to assure the safety and health of students and employees, the College seeks to maintain a work and learning environment free of the unlawful manufacture, distribution, possession or use of a controlled substance or the abuse of alcohol. Drug and alcohol abuse affects the responsible conduct of business, teaching and learning and therefore will not be tolerated.

1.2 This policy is based on the following objectives:

(1) To maintain a safe and healthy environment for students and employees;

(2) To maintain the good reputation of the College and its employees;

(3) To minimize accidental injuries to a person or property;

(4) To keep absenteeism and tardiness at a minimum and to improve the effective performance of job duties and productivity of all employees and the educational performance of all students;

(5) In appropriate circumstances, to assist students and employees in securing substance abuse rehabilitation;

(6) To comply with the federal Drug-Free Workplace Act of 1988, the Drug-Free Schools and Communities Act Amendments of 1989, and other applicable legislation;

(7) To adopt and implement a program to prevent use of illicit drugs and abuse of alcohol by students and employees.

1.3 This policy shall be in addition to any drug abuse policy or policies relating to participation in intercollegiate athletics.

2. Definitions

As used in this policy, the following definitions apply:

2.1 "Drugs or other controlled substances" means any substance, other than alcohol, capable of altering an individual's mood, perception, pain level or judgment.

2.11 A "prescribed drug" is any substance prescribed for individual consumption by a licensed medical practitioner. It includes prescribed drugs and over-the-counter drugs which have been legally obtained and are being used for the purpose for which they were prescribed or manufactured.

2.12 An "illicit drug" or chemical substance is: (a) any drug or chemical substance, the use, sale or possession of which is illegal under any state or federal law, or (b) one which is legally obtainable but has not been legally obtained. The term includes prescribed drugs not legally obtained and prescribed drugs not being used for prescribed purposes.

2.13 "Controlled substance" means a controlled substance in Schedules I–V of Section 202 of the Controlled Substance Act (21 U.S.C.S. 812) or which possession, sale or delivery results in criminal sanctions under the Texas Controlled Substances Act (Art. 4476-15, TCS). In general, this includes all prescription drugs, as well as those substances for which there is no generally accepted medicinal use (e.g., heroin, LSD, marijuana, etc.), and substances which possess a chemical structure similar to that of the controlled substance (e.g., "Designer Drugs"). The term does not include alcohol.

2.2 "Alcohol" refers to any beverage that is "alcohol, or any beverage containing more than one-half of one percent of alcohol by volume, which is capable of use for beverage purposes, either alone or when diluted."

2.3 "Alcohol abuse" means the excessive use of alcohol in a manner that interferes with (1) physical or psychological functioning, (2) social adaptation, (3) educational performance or (4) occupational functioning.

2.4 "Conviction" means a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charged with the responsibility to determine violations of the Federal or State criminal drug statutes. (See 9.5 for time limitations on reporting such convictions.)

2.5 "Cause for reasonable suspicion" is established by (1) observation, (2) action and/or behaviors of the individual, (3) witness by supervisor or other reliable individual of possession or use or (4) any other legal measure used for alcohol or drug detection.2.6 "Criminal drug statute" means a criminal statute involving manufacture, distribution, dispensation, use or possession of any controlled substance.

2.7 "Sanctions" may include completion of an appropriate rehabilitation or assistance program, probation, expulsion, termination or referral to authorities for prosecution. If an employee has been convicted of a criminal drug statute, sanctions must be imposed within 30 days.

3. Policy

3.1 Standards of Conduct: The unlawful manufacture, distribution, possession or use of illicit drugs or alcohol is strictly prohibited.

3.2 Sanctions will be imposed on students and employees (consistent with local, state and federal law), up to and including expulsion or termination of employment and referral for prosecution, for violation of the standards of conduct set forth in 3.1.

Electronic Device Policy

Electronic devices (such as cell phones, MP3 players and laptops) may not be used during tests unless specifically allowed by the instructor, or if the Special Populations Coordinator determines that a device is an acceptable accommodation for a physical or mental disability. Under any other circumstances, the use of an electronic device during a test is considered "academic dishonesty" and will result in appropriate sanctions as outlined in the Instructor's syllabus, the Faculty Handbook (Section IX-1) and the Student Handbook ("Academic Dishonesty").

Use of electronic devices during normal class hours distracts other students, disrupts the class and wastes valuable time. The syllabus for every LSC-PA course includes that instructor's policy regarding the use of electronic devices during class.

Eligibility for Extracurricular Activities

An extracurricular activity is understood to be an activity representing the student body, any student organization, any department or division organization or any general activity representing LSCPA.

Any student currently registered, not on disciplinary or scholastic probation, and who has a GPA of at least 2.0 for both the college work completed at LSCPA and that of the preceding semester is eligible to participate in extracurricular activities. Individual organizations may establish higher requirements for GPA and enrollment status.

For the purpose of establishing eligibility, two six-week summer terms may count as one semester. Transfer students have the same eligibility as freshmen students until completion of one semester.

Hazing

Hazing is prohibited in state educational institutions by the Texas Education Code, Section 4.19. Lamar State College-Port Arthur students are forbidden to engage in, encourage, aid or assist any person(s) participating in what is commonly known and recognized as hazing.

Any student who does so will be subject to college disciplinary action and might also expect to be dealt with by civil authority. Refer to the Student Handbook for more specific definitions and information relevant to the legal implications of hazing.

Non-Smoking Policy

In order to protect the health, safety and welfare of the campus community, the College is committed to providing an environment that limits exposure to the harmful effects of tobacco products.

This commitment derives from two concerns. First, a mounting body of evidence indicates that "second-hand" tobacco smoke can be harmful to non-smokers. Both administrative and judicial decisions hold that an employer's obligation to provide a workplace that is free of known health hazards includes limiting the exposure of non-smokers to tobacco smoke. Second, as an educational institution, Lamar State College-Port Arthur believes it has a responsibility to promote values and practices that contribute to good health. Given the convincing medical evidence of the harmful effects of tobacco use, the College cannot, in good conscience, condone or encourage the use of those products.

I. All campus buildings are designated "smoke free," including all instructional facilities; faculty, staff and administrative offices; and student services areas.

II. The use of smokeless tobacco, including snuff and chewing tobacco, is prohibited on campus.

III. The sale of tobacco products on campus is prohibited.

IV. Smoking is prohibited in campus-owned vehicles available for general use.

V. As used in this policy, the term "smoking" shall include all of the following:

   a. Carrying or holding a lighted pipe, cigar, cigarette or any other lighted smoking equipment or device;

   b. Lighting a pipe, cigar, cigarette or any other smoking equipment or device;

   c. Emitting or exhaling the smoke of a pipe, cigar, cigarette or any other smoking equipment or device.

VI. The terms of this policy will be distributed to all current employees and made available to all prospective employees prior to hiring. The terms of this policy will be distributed to all current students and published in all future editions of the catalog.

Parking Regulations

Each student who pays the necessary fee is issued a hanging tag that permits parking on campus. This tag is numbered and is to be displayed as instructed in official parking and traffic regulations, which are issued when automobiles are registered. It is an important document and should be read thoroughly.

Strict observance of traffic and parking regulations is necessary for the safe, orderly flow of vehicles in the campus area. Designated handicapped parking spaces are available. For information, contact the Vice President for Student Services.

Student Health Insurance

All full-time students enrolled in the College are eligible to purchase health and accident insurance. Coverage may be purchased for an entire year or on a semester basis and is available to students only or students and their dependents. The fees for the year may be paid upon enrollment or during the academic year. A brochure explaining the coverage, cost and benefits is available in the Student Activities Office. Proof of health and accident insurance is required of all foreign students and all participants in intramural/recreational sports programs.

Student Travel Policies

Student Travel Authorization and Supervision

Each college-related activity that requires student travel must be authorized by the sponsoring department's Dean or Department Chair. The authorizing Dean or Department Chair must designate a faculty/staff member or members to be responsible for the safety and conduct of the trip. (Exception): Student employees of the College, in the course of their employment, may be drivers on and in the vicinity of campus.

Use of Students as Drivers

Only persons meeting the college's polices defining "Employee" and who hold an "Approved Driver Certificate" from Lamar State College-Port Arthur are eligible to drive. Students, except student employees driving as part of their employment with the College, are expressly excluded from operating college vehicles.

Insurance Requirements for Transporting Students

Passengers Involved in College-Related Activities – The trip sponsor is responsible for each student who is to be a passenger in a vehicle driven on a college-related activity. All student travel must be noted to the Director of Student Activities and Vice President for Student Services prior to the trip for special event insurance that is available.

If students are to be transported in rental vehicles, the college, through the State of Texas, has several rental sources that offer special rate and inclusive insurance for this type of travel at no or little additional cost. To use this the sponsor must use their State Travel Card with our agency code located on it to rent transportation. Without the State Travel Card a sponsor must contact the Travel Coordinator in the Business Office to make such reservations and rental for the trip. If students are to be transported in rental vehicles on the sponsor's personal payment, personal injury and personal effects insurance should be purchased as part of the vehicle rental agreement. This is particularly important where vans or buses are rented to transport a large number of students in a single vehicle.

Each student who travels by motor vehicle or any other form of transportation to participate in a college-related activity, including but not limited to academically related field trips or courses, competitions or contest; or non-academic activities such as those sponsored by Student Services or team sports, must execute a copy of the Release and Indemnification Agreement and Authorization for Emergency Medical Treatment. Copies of these documents are available from the Student Activities Director.

If students use their own vehicles to drive themselves or transport other students as passengers to college-related activities, they should be informed in advance that their personal insurance will be responsible for any liability arising from the trip.

All College travel guidelines are presented in the college's Vehicle Fleet Management Plan and all should familiarize themselves with these and other critical travel policies and procedures. It can be located on the College website under the Physical Plant Department.

Guidelines for Transporting Students Involved in College-Related Activities

Loading of the vehicle shall be done in accordance with the vehicle manufacturer's recommendations. Particular attention should be paid in loading the large (3/4 ton) vans. No more than eleven (11) passengers should be transported and even with a reduced load the driver must remain cautious when maneuvering or making quick turns in order to avoid a rollover.

All occupants must remain seated with their seat belts fastened while the vehicle is in motion. The number of occupants must never exceed the number of working seat belts in the vehicle.

The use of tobacco products is not allowed in any vehicles owned by the College.

The Trip Manifest, Itinerary and Authorization for Student Travel documents must be verified by the LSC-PA sponsor of the trip and the driver.

Each vehicle transporting students involved in college-related activities shall be equipped with the following items: a first aid kit, a fire extinguisher, a flashlight, water, a Texas state map, a cellular telephone and a Voyager Fleet credit card.

Student trips will be planned in accordance with the following restrictions:

- The driver may not drive more than eight hours in any calendar day.

- The driver may not drive more than 48 hours in a week.
- Every driver must take a rest period of at least 12 hours between driving periods.
- The maximum number of hours any passenger car or van may be driven during any calendar day is 12 hours.

Student Conduct

To meet its educational objectives, an institution of higher learning must expect rational, mature behavior from its constituency. To accept anything less invites the destruction of not only academic freedom, but also the system of higher education.

Student discipline at Lamar State College-Port Arthur is based on an educational philosophy of helping students grow and mature into responsible citizens. When a student behaves in a manner that requires disciplinary action, a careful investigation of all facts is made and the student is afforded every opportunity to assist in arriving at a just and equitable decision.

Counseling, conferences with parents and/or instructors, conferences with peer groups and other techniques as may seem appropriate, may be employed in making discipline an educational experience.

Student Complaint Procedure Texas Higher Education Coordinating Board[1]

Definitions

The following words and terms, when used in this subchapter, shall have the following meaning, unless the context clearly indicates otherwise:
(1) Agency - Texas Higher Education Coordinating Board.
(2) Commissioner - The Commissioner of Higher Education.
(3) Complainant or student - A current, former, or prospective student of an institution who submits a complaint to the Agency regarding that institution.
(4) Educational association - Independent Colleges and Universities of Texas, Inc. (ICUT).
(5) Institution - A public or private (non-profit, not-for-profit, or for-profit) institution of higher education that the Legislature or the Agency has authorized to operate in Texas.
(6) Student complaint form - A standard form, available in downloadable format on the Agency's website or in hard copy form from the Agency, which is required to be used in filing any student complaint with the Agency.
Source Note: The provisions of this §1.110 adopted to be effective November 28, 2012, 37 TexReg 9353

Scope and Purpose

(a) This subchapter shall govern all instances in which complainants file written complaints with the Agency regarding institutions.
(b) This subchapter implements Texas Education Code, §61.031, concerning Public Interest Information and Complaints, and 34 C.F.R. §600.9(a)(1) of the United States Department of Education's Program Integrity regulations, which requires each state to establish "a process to review and appropriately act on complaints concerning an institution of higher education including enforcing applicable State laws."
(c) The purpose of this subchapter is:
(1) to encourage the early resolution of student complaints through use of the institutions' grievance procedures or informal processes in appropriate cases; and
(2) to establish procedures for the administration of all student complaints filed with the Agency.
Source Note: The provisions of this §1.111 adopted to be effective November 28, 2012, 37 TexReg 9353

Complaints Not Reviewed by the Agency

The following is a non-exhaustive list of student complaints that are not reviewed by the Agency:
(1) The Agency does not handle, investigate, or attempt to resolve anonymous complaints.
(2) The Agency does not intervene in matters solely concerning an individual's grades or examination results, as these are within the sole purview of the institution and its faculty.
(3) The Agency does not intervene in matters solely related to student life such as student housing, dining facilities, food service, violations of the student code of conduct, or student activities and organizations, as these issues are within the sole purview of the institution.
(4) The Agency does not handle, investigate, or attempt to resolve complaints in matters that are or have been in litigation.
(5) The Agency does not handle, investigate, or attempt to resolve complaints about religious institutions relating solely to their religious (as opposed to secular) standards and religious programs of study.
(6) The Agency does not handle, investigate, or attempt to resolve student complaints against institutions not authorized by the Agency to operate in Texas. Institutions authorized by the Agency to operate in Texas are listed on the following websites: http://www.txhighereddata.org and http://www.thecb.state.tx.us.
(7) The Agency does not handle, investigate, or attempt to resolve complaints regarding tribal institutions.
(8) The Agency does not handle, investigate, or attempt to resolve complaints about criminal matters, and instead encourages students to contact local law enforcement authorities regarding these complaints.
Source Note: The provisions of this §1.113 adopted to be effective November 28, 2012, 37 TexReg 9353

[1] Texas Administrative Code

Filing a Complaint

(a) The student complaint form is available on the Agency's website. All complaints must be submitted to the Agency on the student complaint form.
(b) Complainants shall send student complaint forms by electronic mail to StudentComplaints@thecb.state.tx.us or by mail to the Texas Higher Education Coordinating Board, Office of the General Counsel, P.O. Box 12788, Austin, Texas 78711-2788. Facsimile transmissions of the student complaint form are not accepted.
(c) All submitted complaints must include a student complaint form and a signed Family Educational Rights and Privacy Act (FERPA) Consent and Release form, which is at the bottom of the student complaint form. Submitted complaints regarding students with disabilities shall also include a signed Authorization to Disclose Medical Record Information form, which is at the bottom of the student complaint form.
(d) The Agency does not handle, investigate, or attempt to resolve complaints concerning actions that occurred more than two years prior to filing a student complaint form with the Agency, unless the cause of the delay in filing the student complaint form with the Agency was the complainant's exhaustion of the institution's grievance procedures.
(e) Former students shall file a student complaint form with the Agency no later than one year after the student's last date of attendance at the institution, or within six months of discovering the grounds for complaint, unless the cause of the delay in filing the student complaint form with the Agency was the complainant's exhaustion of the institution's grievance procedures.
Source Note: The provisions of this §1.114 adopted to be effective November 28, 2012, 37 TexReg 9353

Attempt to Facilitate an Informal Resolution to the Complaint

During the investigation of a student complaint, Agency staff shall, in appropriate cases, attempt to facilitate an informal resolution to the complaint that is mutually satisfactory to the complainant and institution.
Source Note: The provisions of this §1.117 adopted to be effective November 28, 2012, 37 TexReg 9353

Recommendation for Resolution Made to the Commissioner

In cases in which an informal resolution between the complainant and institution is not feasible, Agency staff shall evaluate the results of the investigation of the student complaint and recommend a course of action to the Commissioner. If Agency staff finds the complaint to be without merit following the investigation, Agency staff shall recommend that the complaint be dismissed. If Agency staff finds the complaint has merit following the investigation, Agency staff may recommend that the Commissioner require the institution to take specific action(s) to remedy the complaint.
Source Note: The provisions of this §1.118 adopted to be effective November 28, 2012, 37 TexReg 9353

Written Determination of the Commissioner

After receiving the Agency staff's recommendation, the Commissioner shall consider the recommendation regarding the complaint and render a written determination. If the Commissioner finds the complaint is without merit, the Commissioner shall dismiss the complaint. If the Commissioner finds the complaint has merit, the Commissioner may require the institution to take specific action(s) to remedy the complaint. In the Commissioner's sole discretion, complaints regarding institutional integrity may be forwarded to the Board for its consideration and determination. The Agency shall send a copy of the Commissioner's or the Board's written determination to the complainant and the institution. The Agency may take all appropriate actions to enforce its determination.
Source Note: The provisions of this §1.119 adopted to be effective November 28, 2012, 37 TexReg 9353

Authority of the Commissioner to Issue Written Determinations Regarding Student Complaints

With regard to student complaints to the Board about a public or private (non-profit, not-for-profit, or for-profit) institution of higher education that the legislature or the Agency has authorized to operate in Texas, the Board authorizes the Commissioner to issue written determinations dismissing complaints or requiring institutions to take specific action(s) to remedy complaints. In the Commissioner's sole discretion, complaints regarding institutional integrity may be forwarded to the Board for its consideration and determination. The student complaint procedure is set out in this subchapter.
Source Note: The provisions of this §1.120 adopted to be effective November 28, 2012, 37 TexReg 9353

Other Services

Alumni Association

The Alumni Association, which includes former students, current and former employees and friends of the College, supports the school and provides six student scholarships every academic year. The group's activities include an annual picnic with college employees and an annual banquet meeting in October.

The association traces its beginning to the Port Arthur College Alumni Association organized in 1917 and active until the early 1950s. In 1986, with the encouragement of Lamar-Port Arthur President Sam Monroe, former PACAA members, faculty and staff reactivated the group as the Lamar University-Port Arthur Alumni Association. The organization changed its name in 2000 to reflect the change of the institution's name.

Campus Security

Community Service officers help to provide a safe environment for students, visitors and college employees. They provide escort service to vehicles upon request and provide parking lot surveillance. The College also utilizes video and other forms of surveillance to aid in providing a secure and safe operation. The campus also relies on the Port Arthur Police Department when in need.

Campus emergencies must be reported to the Security Office by dialing '0'. During evening hours contact the campus operator by dialing '0'.

Counseling Services

Lamar State College-Port Arthur recognizes that stressful personal and family problems can have an adverse impact on the academic performance of college students. While no program can eliminate all personal problems, efforts to provide timely assessment and effective counseling are steps that can be taken to address such concerns. In an effort to provide support in this area, Student Services offers assistance to students in the form of personal counseling to help students confront and cope with today's problems.

Counseling services referral can be arranged for students by contacting the Vice President for Student Services.

Fitness Center

Lamar State College Port Arthur has a state of the art fitness center composed of cardiovascular machines such as treadmills, bikes and rowing machines as well as strength training equipment such as free weights and Pre-Cor weight machines. A dance studio is adjacent to the Fitness Center where classes are offered. The basketball court is available for free play. The Fitness Center is student-driven and works with the interests of the student body to form such things as basketball contests, fun runs and club/intramural sports activities.

The Fitness Center is located in the Carl Parker Building.

Port Arthur Higher Education Foundation

Far-sighted leaders formed the Port Arthur Higher Education Foundation as a 501(c) (3) non-profit organization in 1973. Its purpose is to promote the arts, sciences and programs of Port Arthur College, which later became Lamar State College-Port Arthur.

The Foundation's early role included assisting the College in acquiring property surrounding the campus and in making special contributions, such as providing $125,000 to purchase books for the Gates Memorial Library after city voters donated the library to the College.

The Foundation's current primary purpose is to administer more than $5 million in permanently endowed scholarships for Lamar State College-Port Arthur students. The awards bear the names of longtime community members, celebrities and local social and civic clubs, including Robert Rauschenberg, H.S. and Bernice B. Anderson, Lloyd and Joe Hayes, Sydalise Fredeman, G.W. Bailey and the Port Arthur Rotary Club.

Lamar State College-Port Arthur receives applications for the foundation's scholarships, which may be awarded based on academic merit, financial need or both.

Intercollegiate Athletics

The College also has a Division I intercollegiate athletic programs; men's basketball and women's softball. The teams compete in Region XIV, a conference of the National Junior College Athletic Association (NJCAA). Region Xiv is known as one of the strongest conferences in the NJCAA.

Men's Basketball

Lamar State College Port Arthur sponsors a Men's Basketball Team that competes in NJCAA Division I. Each year, approximately 14 student-athletes represent the Seahawks playing some of the best teams in the country. In 2011, the Seahawk Basketball team earned a spot in the National NJCAA Basketball Tournament by winning the Region XIV Tournament. Students interested in participating should contact the Head Basketball Coach.

Women's Softball

Lamar State College Port Arthur sponsors a Women's Softball ball Team that competes in NJCAA Division I. Each year, approximately 20 student-athletes represent the Seahawks playing teams from Texas to Florida. Each year there are approximately 25 home games that Lamar State Students can cheer on the home team! Students interested in participating should contact the Head Softball Coach.

Student Support

Students interested in a career in athletics can get first-hand experience assisting the coaches and staff. Students may gain experience in such areas as operations, marketing, tutoring and coaching. Students interested in participating should contact the Director of Athletics.

Club Sports

Lamar State College Port Arthur is committed to providing student life experiences to our students. When students show an interest in forming a club sports team, the Fitness Center Staff work with the student group to help achieve the students' goals.

Club sports are designed to meet the competitive athletic desires of students, faculty and staff. Many student athletes choose Club Sports because their sport is not offered through the varsity or they do not wish to make the time commitment necessary for a varsity sport. Club Sports competes against other institutions of higher education from the local and regional area on a non-varsity level. Each Club Sports Team is a registered student organization providing instruction, organizing practice and scheduling competition in a specific sport. As a student organization each team is administered, developed and coached by students on that team. Teams may have larger or fewer members based on the level of interest in that sport. Club Sports are partially funded through the College, and no athletes are on scholarships.

Technology Services

Technology Services provides services to students who attend Lamar State College Port Arthur. The services include student e-mail, internet connectivity from all the computer labs on campus, access to our learning management system, access to Self Service Banner, distance education support, registration, and additional services as needed.

Educational Programs

Academic and Technical Programs

Lamar State College-Port Arthur offers general academic courses that lead to Associate of Arts and Associate of Arts in Teaching degrees. Courses for transfer to four-year institutions are offered in accounting, economics, anthropology, art, government, home economics, kinesiology, physics, history, speech, computer science, health, mathematics, psychology, biology, chemistry, geography, geology, sociology, criminal justice, music, drama, English, teaching and Spanish.

Students can complete two full years of course work and satisfy the majority of the general education requirements for a bachelor's degree.

Students can complete freshman and sophomore course work at Lamar State College- Port Arthur and be prepared to move into junior and senior level course work at a four-year institution.

Lamar State College-Port Arthur offers a technical education curriculum that leads to an Associate of Applied Science Degree in office administration, commercial music: performance, commercial music: sound engineer, audiovisual production, cosmetology,