

POLICY: ETHICS
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.0
REVISED: OCTOBER 2004; DECEMBER 2005

1. CODE OF ETHICS

Lamar State College – Port Arthur is committed to the highest standards of ethics, integrity, and fairness in all dealings and to provide the public with the utmost level of confidence in our organization, educational services, administrative business processes, and financial data. The College is in a position of trust with respect to many external organizations and agencies. Accordingly, all College personnel have a responsibility to the government, donors, parents and student to use its funds prudently, ethically, and for the purposes for which they are designed.

1.1 ETHICS is defined as the principals of conduct governing an individual or group.

1.2 PREAMBLE

Ethics and integrity are the responsibility of each individual. Therefore, every member of the faculty and staff, any other person acting on behalf of the College is responsible for ethical conduct consistent with the Code. As such, College administration, faculty, deans, department chairs, and others in supervisory positions must assume responsibility for ensuring that their conduct, and the conduct of those they supervise, complies with this Code. Business activities undertaken on behalf of LSC-PA with the public, the government, suppliers, students and one another must reflect the highest standards of honesty, integrity, and fairness. Each individual must be especially careful to avoid even the appearance of misconduct or impropriety.

1.3 INTEGRITY

All employees must:

- Perform their work with honesty, objectivity, diligence, and responsibility.
- Act with a high level of prudence and due professional care avoiding any real or apparent conflicts of interest.
- Act in good faith without misrepresenting material facts or allowing their independent judgment to be subordinated.
- Accord respect to self and others and accept responsibility for all actions.
- Observe the law and make disclosures expected by the law.
- Not knowingly be a party to any illegal activity or engage in acts that are discreditable to the College.
- Comply with all College policies and procedures.
- Proactively promote ethical behavior amongst peers, in the work environment, and the community.
- Exercise responsible use and control over all College assets and resources.
- Respect and contribute to the legitimate and ethical objectives of the College.
- Accept and respect diversity in our community and adherence to the College's Affirmative Action and Non-discrimination policy.

1.4 GRATUITIES AND "KICKBACKS"

Lamar State College – Port Arthur personnel shall not use their position to secure special privileges for themselves or their close relatives. (see definition below under "*Nepotism*"). Employees shall not give, offer or promise anything of value to anyone to enhance relations with that individual or their firm, regardless of whether that individual is in a position to influence any decisions with respect to the College or its activities. This includes, but is not limited to, entertainment, meals, refreshments, gratuities or gifts, loans, rewards, compensation, or other monetary remuneration. This also applies to all contractors, subcontractors, and/or vendors for the purpose of improperly obtaining or receiving favorable treatment. Nor shall any LSC-PA personnel solicit or accept anything of value from any governmental official, contractor, subcontractor, vendor or others for such a purpose.

1.5 CONFLICT OF INTEREST

All employees must ensure that no conflicts of interest exist. The College administration has an obligation, in accordance with Board Statutes, to ensure that employees avoid conflicts of interest and to assure that the activities and interests of its employees do not conflict with their obligations to the institution or its well-being. A conflict of interest arises when employees place themselves in a position where they could use their position to create benefits for their private interests or to give improper advantage to others. When an employee has a significant interest in, or a consulting arrangement with, a private business concern, it is important that they avoid conflicts of interest. Employees are encouraged to direct inquiries relative to conflict of interest concerns to their department head and/or division executive officers. In those situations where a possible conflict of interest may occur, management shall take action which may include relieving the employee of the assignment and assigning the matter to another qualified employee who does not have a conflict of interest.

1.6 CONFLICT OF COMMITMENT

With the acceptance of a full-time at LSC-PA, every employee is expected to accord the College their primary professional loyalty and to arrange outside obligations, financial interest, and activities so as not to conflict with their overriding commitment to the College. Consultants are also expected to arrange their outside obligations and activities so as not to conflict with their contracted commitment to the College.

A conflict of commitment occurs when an employee's involvement in external activities adversely affects their capacity to meet their primary obligation to the College due to a perceptible reduction of the individual's time and energy devoted to LSC-PA activities. Departments may permit certain outside activities, with appropriate notice to and written approval by the appropriate department head, so long as these endeavors do not interfere with an employee's obligations to the College.

1.7 NEPOTISM

Blood or marital relationships with other College employees are not regarded as a deterrent to appointment, reassignment or continuance in a present position. Close relatives may not be employed where one is in a position of influence over another. Close relatives include husband or wife, parent or child, son-in-law, daughter-in-law, brothers or sisters. A position of influence exists in instances where selection for employment, judgments concerning performance, compensation, status, fitness for promotion or discipline/discharge, require the action of one person with respect to the other.

1.8 CONFIDENTIALITY

Security and confidentiality of College records are matters of concern for all employees who have access to manual or computerized information and files. Each person working with College information holds a position of trust and must recognize the responsibilities of preserving the security and confidentiality of the information, any employee or person with authorized access to the system is expected:

- Not to make or permit unauthorized use of any information or files.
- Not to seek personal benefit or permit others to benefit personally by any confidential information which has come to them through their work assignment.
- Not to exhibit or divulge the contents of any record or report to any person except in the conduct of their regular work assignment.
- Not to remove any official record of report (or copy) from the office where it is kept except in performance of regular duties or in cases with prior approval.
- Not to operate or request others to operate any College data processing equipment for personal business.

- Not to aid, abet or act in conspiracy with any other person to violate any part of this code; and,
- To immediately report any violation of this code to management.

1.9 COMPETENCY

All employees have an obligation to execute their duties and responsibilities with professional care and skill to the best of their knowledge and abilities. To that end, all employees must familiarize themselves with the appropriate College and/or department policies and procedures, applicable laws and regulations, and other rules as required to perform their respective jobs.

1.10 FINANCIAL REPORTING

All College accounts, financial reports, tax returns, expense reimbursement, time sheets and other documents, including those submitted to government agency's, must be accurate, clear, timely, and complete. All entries in College books and records, including departmental accounts, and individual expense reports, must accurately reflect each transaction. It is unlawful for any employee to take an action to fraudulently influence, coerce, manipulate, or mislead an auditor engaged in the performance of an audit for the purpose of rendering the financial statements materially misleading.

1.11 REPORTING CODE VIOLATIONS

Employees should report suspected violations of this Code, applicable laws, regulations, and government grant and contract requirements through standard management reporting channels, beginning with the immediate supervisor. Alternatively, employees may go to a higher level of management and may also report suspected violations or problems to the Director of Internal Audit. In all instances, violations of laws or regulations should be reported to the Director of Internal Audit (880-8933). Such reports may be made confidentially and/or anonymously although a greater level of information allows for a more thorough investigation. Raising such concerns is a service to the College and consistent with the State of Texas's Whistleblowers' Protection Act, will not jeopardize employment.

The Texas State University System has selected a private contractor, EthicsPoint, as a confidential means of reporting for individuals unable to use existing reporting procedures. A link is found on the TSUS web site

All employees should cooperate fully in the investigation of any misconduct.

1.12 CONSEQUENCES OF VIOLATION

Each person is responsible for ensuring that their own conduct, and the conduct of anyone reporting to them, fully complies with this Code and with the College's policies. Violations will result in appropriate disciplinary action up to and including discharge from employment. Disciplinary action will be taken in accordance with the procedures applicable to faculty or staff as codified in the respective Faculty Handbook and in this Administrative Policy and Procedure. Conduct representing a violation of the Code may, in some circumstances, also subject an individual to civil or criminal charges and penalties.

1.13 PROHIBITED ACTIONS OF EMPLOYEES

An employee of Lamar State College - Port Arthur shall not:

- Accept or solicit any gift, favor or service that might reasonably tend to influence the employee in the discharge of official duties.
- Use an official position to secure special privileges or exemptions for the employee or others, except as may be otherwise authorized by law.
- Accept employment or engage in any business or professional activity which might reasonably be expected to require or induce the employee to disclose confidential information acquired by reason of such employee's official position or impair the employee's independence of judgment in the performance of public duties.

- Disclose confidential information gained by reason of one's employment, or otherwise use such information for personal gain or benefit.
- Transact any business in an official capacity with any business entity of which the employee is an officer, agent, or member or in which the employee owns a controlling interest unless the Board of Regents has reviewed the matter and determined no conflict of interest exists.
- Make personal investments in any enterprise which could reasonably be expected to create a substantial conflict between the private interests of the employee and the public interests of his or her employee.
- Receive any compensation for services as a state employee from any source other than the State of Texas, except as otherwise provided by law.
- Engage in any form of sexual harassment or racial harassment as defined in the Administrative Policies and Procedures Manual.

2. TRAINING

The System Administrative Office shall conduct, in even numbered years, training sessions for the personnel of each component institution responsible for ethics training in the various departments of such institutions. These training sessions will provide the trainees with the methods, policies and materials necessary to allow them to train each employee within their supervision or responsibility. Each component institution is responsible for training each employee each biennium. The President will notify the Chancellor upon completion of the ethics training each biennium.

3. CERTIFICATION STATEMENT

This APP has been approved by the following individuals in their official capacities and represents Lamar State College - Port Arthur policy and procedure from the date of this document until superseded.

Dr. Sam Monroe, President
 Gwen Reck, Vice President Finance, College Fraud Officer
 Linda McGee, Director Human Resources

POLICY: STANDARDS OF CONDUCT
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.1
REVISED: OCTOBER 2004; DECEMBER 2005

1. State law requires that all individuals who are responsible to the State in the performance of their official duties must observe certain standards of conduct and disclosure requirements.

Employees and officers may not:

- accepts or solicits any gift, favor, or service that might reasonably tend to influence the employee in the discharge of official duties or that the employee knows or should know is being offered with the intent to influence the employee's official conduct;
- accepts other employment or engages in a business or professional activity that the employee might reasonably expect would require or induce the employee to disclose confidential information acquired by reason of the official position;
- accepts other employment or compensation that could reasonably be expected to impair the employee's independence of judgment in the performance of the employee's official duties;
- makes personal investments that could reasonably be expected to create a substantial conflict between the employee's private interest and the public interest; or
- intentionally or knowingly solicits, accepts, or agrees to accept any benefit for having exercised the employee's official powers or performed the employee's official duties in favor of another.

2. TRAVEL EXPENSES AND ALLOWANCES

2.1 Transportation, Meals, and Lodging

Employees of Lamar State College - Port Arthur are entitled to receive the following when traveling to conduct official business:

1. Actual costs of lodging and meals for in-state travel, except that such reimbursements may not exceed the current maximum established by law.
2. For out-of-state travel, employees may receive actual costs for lodging and a per diem for meals not to exceed the locality-based allowance provided by the Federal Travel Regulations for lodging and meals unless the State Comptroller determines in advance of the travel that local conditions warrant a change in the lodging rate for a particular location.

2.2 Purpose of Travel

To qualify for travel reimbursements the purpose of a trip must be "state business" or "official business" of the College. State or official business is the accomplishment of a governmental function directly entrusted to Lamar State College - Port Arthur, including the reasonably necessary means and methods to accomplish that function.

2.3 Improper Travel Reimbursement

When an employee engages in travel for which compensation is to be received from any source other than Lamar State College - Port Arthur funds, he or she shall not submit a claim under the provisions of the Lamar State College - Port Arthur travel regulations. An employee who receives an overpayment for a travel expense shall reimburse Lamar State College - Port Arthur for the overpayment.

2.4 Travel Bonus (Frequent Flyer) Awards

Employees who earn credit with airlines, hotels, car rental companies, etc. for official travel are not required to account for such credit or to use such for official travel only.

2.5 Official Travel by Spouses and Relatives of Employees

Spouses and other relatives of employees may qualify to have travel expenses paid by Lamar State College - Port Arthur if their presence at a function or on a trip is for an official purpose benefiting Lamar State College - Port Arthur and/or the State of Texas. In making a determination of whether the presence of a spouse or relative is for an official purpose, the factors to be considered are the nature and duties of the employee's office, the traditional role, if any, of the spouse or relative, the purpose of the particular trip, and the spouse or relative's connection with that purpose.

2.6 Foreign Travel

A request by an employee for travel outside of the United States, excluding Mexico or Canada, must be approved by the Chancellor and the Governor's office 30 days in advance. Forms and procedures prescribed by the Governor's office shall be utilized.

2.7 Reimbursement of Expense

Verified expense accounts shall be submitted to the appropriate college official for processing and the same shall be subject to review.

3. TRAINING

The System Administrative Office shall conduct, in even numbered years, training sessions for the personnel of each component institution responsible for ethics training in the various departments of such institutions. These training sessions will provide the trainees with the methods, policies and materials necessary to allow them to train each employee within their supervision or responsibility. Each component institution is responsible for training each employee each biennium. The President will notify the Chancellor upon completion of the ethics training each biennium.

4. CERTIFICATION STATEMENT

This APP has been approved by the following individuals in their official capacities and represents Lamar State College - Port Arthur policy and procedure from the date of this document until superseded.

Dr. Sam Monroe, President
Gwen Reck, Vice President Finance, College Fraud Officer
Linda McGee, Director Human Resources

POLICY: CONFLICTS OF INTEREST
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.2
REVISED: OCTOBER 2004; DECEMBER 2005

1. CONFLICTS OF INTEREST

1.1 Ethics Commission Financial Disclosure Statements

The President shall file a financial statement with the Texas Ethics Commission not later than April 30 each year in which the President has served in such capacity for any portion of the immediately preceding twelve (12) months on forms prescribed by the commission.

1.2 Contracts Prohibited

Except as provided below, neither the Texas State University System nor Lamar State College - Port Arthur may enter into a contract in which a Regent or the Regent's spouse has a direct or indirect pecuniary interest.

1.3 Benefits, Gifts and Honoraria

A "benefit" is anything reasonably regarded as pecuniary gain or pecuniary advantage, including benefit to any other person in whose welfare an employee has a direct and substantial interest.

1.4 Bribery

An employee shall not solicit, offer, or accept any benefit in exchange for his or her decision, opinion, recommendation, vote, or other exercise of official power or discretion.

1.5 Prohibited Benefits

An employee shall not solicit, accept, or agree to accept any benefit from any person the employee knows is interested in or is likely to become interested in any contract, purchase, payment, claim, or transaction involving the employee's discretion. This prohibition does not apply to (1) gifts or other benefits conferred on account of kinship or a personal, professional, or business relationship independent of an employee's status, respectively, as an employee; (2) a fee prescribed by law to be received by an employee or any other benefit to which he or she is lawfully entitled or for which he or she gives legitimate consideration in a capacity other than as an employee of Lamar State College - Port Arthur; (3) a gift, award, or memento that is received from a lobbyist who is required to make reports under Chapter 305 of the Government Code; and, (4) items having a value of less than \$50, not including cash or negotiable instruments. An employee who receives an unsolicited benefit that he or she is prohibited from accepting by law may donate the benefit to a governmental entity that has the authority to accept the gift or may donate the benefit to a recognized tax-exempt charitable organization formed for education, religious, or scientific purposes.

1.6 Food, Lodging, Transportation, and Entertainment Received as a Guest

An employee may accept food, lodging, transportation, or entertainment from persons or entities he or she knows or reasonably should know are interested in or likely to become interested in a contract, purchase, payment, claim, decision, or transaction involving the exercise of the Board's discretion only if the employee is a "guest" as defined by Texas law. An employee is a "guest" if the person or a representative of the entity providing the food, lodging, transportation, or entertainment is present at the time the food, lodging, transportation, or entertainment is received or enjoyed by the employee. The President is required to report any such benefits valued at over \$250 on his annual disclosure statements filed with the Texas Ethics Commission.

1.7 Gifts or Benefits from Friends, Relatives, and Associates

Employees may accept gifts or benefits from personal friends, relatives, or business associates with whom they have a relationship independent of their official status, so long as the benefit is not offered in exchange for official action or decision.

1.8 Awards

Employees may accept plaques and similar recognition awards.

1.9 Honoraria

Employees may not solicit, accept, or agree to accept an honorarium in consideration for services they would not have been asked to provide but for their official position or duties. This prohibition includes a request for or acceptance of a payment made to a third party if made in exchange for such services. However, they may accept the direct provision of or reimbursement for expenses for transportation and lodging incurred in connection with a speaking engagement at a conference or similar event, provided the employee's participation is more than merely perfunctory. Meals provided as a part of the event or reimbursement for actual expenses for meals may also be accepted.

2. POLITICAL ACTIVITIES

2.1 Entertainment

If an employee provides tickets to a public official to allow the official and/or his guests to attend an event, an officer or employee of the System or Lamar State College - Port Arthur will serve as host to the official, and must attend the event.

2.2 Perishable Food Items

Employees may provide public officials with small, infrequent gifts of perishable food items delivered to their offices. These are not considered to be "benefits" for purposes of the provisions of the Penal Code prohibiting such.

2.3 Expenses for Public Officials

Lamar State College - Port Arthur may pay expenses in order to furnish information to state officials relevant to their official position, including presentations about the programs and services of the Texas State University System and its component institutions.

2.4 Use of Official Authority Prohibited

No Lamar State College - Port Arthur employee may use his or her official authority or influence, or permit the use of a program administered by the System to interfere with or affect the result of an election or nomination of a candidate or to achieve any other political purpose. No Lamar State College - Port Arthur employee may do any act or attempt to interfere with anyone who seeks to pay, lend, or contribute private funds or private property to a person or political organization for political purposes. Any employee who violates either of these provisions is subject to immediate termination of employment in accordance with the Texas Government Code.

2.5 Use of System Funds or Property

No Lamar State College - Port Arthur employee shall expend or authorize the expenditure of any System or Lamar State College - Port Arthur funds for the purpose of influencing the outcome of any election, or the passage or defeat of any legislative measure. No System or Lamar State College - Port Arthur funds may be expended for the payment of full or partial salary of any employee who is also the paid lobbyist of any individual, firm, association, or corporation. System and Lamar State College - Port Arthur facilities may be used as polling places for local, state, and national elections.

2.6 Voting and Political Participation

As employees of the State of Texas, Lamar State College - Port Arthur employees have the rights of freedom of association and political participation guaranteed by the state and federal constitutions, except as limited by valid state laws. Lamar State College - Port Arthur employees shall be allowed sufficient time off to vote in public elections without a deduction from pay or from accrued leave time.

2.7 Political Campaign Events on System Property

The Chief Executive Officer of Lamar State College - Port Arthur shall be responsible for promulgating rules for the regulation of political campaign meetings or speeches and other activities relating to political campaigns on property under their control. Such regulations shall be implemented by the Chancellor after approval by the Board of Regents.

2.8 Employees as Candidates and Officeholders

Lamar State College - Port Arthur employees may run for election and serve as members of the governing bodies of school districts, cities, towns, or other local governmental districts. No campaign activities may be conducted during official business hours unless the employee has requested and received permission to use leave time for such purpose. Any employee elected to such a position may not receive any salary for serving as a member of such governing body.

2.9 Political Contributions for Employees

Lamar State College - Port Arthur employees may make personal contributions to candidates for office and political organizations, with the exception that no state employee may contribute personal services, money, or goods of value to a candidate campaigning for speaker of the Texas House of Representatives.

3. DUAL OFFICE HOLDING

3.1 Non-elective State or Federal Office

Lamar State College - Port Arthur employees may hold non-elective offices with boards, commissions, and other state and federal entities provided that the holding of such office, (1) is of benefit to the State of Texas, or is required by state or federal law, and (2) is not in conflict with the employee's position. Such appointments must be approved by the President. Prior to the President's accepting an invitation to serve in an additional non-elective office, the Board of Regents must determine that the appointment meets the two requirements stated above. The Board must also make an official record of any compensation to be received by the President from such appointment, including salary, bonus, per diem or other types of compensation.

3.2 Positions of Employment with Government Agencies

Lamar State College - Port Arthur employees may hold other positions of employment with agencies, boards, commissions, or other entities of government so long as the holding of such positions is consistent with the prohibitions against dual office holding in the Texas Constitution. Special rules for multiple employments with the State are provided in Article IX, Sec. 9, of the General Appropriations Act. The person seeking dual employment must be informed of the special rules before that person becomes employed by more than one agency or institution. Consulting arrangements with federal, state, or local governmental agencies of a detached and independent advisory nature are not considered to be appointments with such agencies.

4. THIRD PARTIES

In accordance with Texas Government Code, Title 10, Subtitle D, Section 2155.003, (<http://www.capitol.state.tx.us/statutes/statutes.html>)

2155.003. CONFLICT OF INTEREST.

- (1) A commission member, employee, or appointee may not:
 - a. Have an interest in, or in any manner be connected with, a contract or bid for a purchase of goods or services by an agency of the state;
 - b. In any manner, including by rebate or gift, accept or receive from a person to whom a contract may be awarded, directly or indirectly, anything of value or a promise, obligation, or contract for future reward or compensation.

(2) A commission member, employee, or appointee who violates Subsection (a)(2) is subject to dismissal.

LSCPA requires that all employees of the college who have been delegated the authority to purchase for the state of Texas must sign a Conflict of Interest statement each year .

5. TRAINING

The System Administrative Office shall conduct, in even numbered years, training sessions for the personnel of each component institution responsible for ethics training in the various departments of such institutions. These training sessions will provide the trainees with the methods, policies and materials necessary to allow them to train each employee within their supervision or responsibility. Each component institution is responsible for training each employee each biennium. The President will notify the Chancellor upon completion of the ethics training each biennium.

6. CERTIFICATION STATEMENT

This APP has been approved by the following individuals in their official capacities and represents Lamar State College - Port Arthur policy and procedure from the date of this document until superseded.

Dr. Sam Monroe, President
Gwen Reck, Vice President Finance, College Fraud Officer
Linda McGee, Director Human Resources

POLICY: FRAUD
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.3
APPROVED: May 2006

1. FRAUD

1.1 This policy is to specifically address fraudulent acts. Fraudulent activity of any kind, including for the benefit of the College, is expressly forbidden. This policy establishes the procedures and responsibilities for reporting and resolving instances of known or suspected fraudulent acts.

1.2 DEFINITION

An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury. Any kind of artifice employed by one person to deceive another. (Black's Law Dictionary)

1.3 BROADENED DEFINITION

For purposes of this policy, the definition has been broadened to include:

- a. an intentional or deliberate act;
- b. depriving the College or a person of something of value or gaining an unfair benefit; and
- c. using deception, false suggestions, suppression of truth, or other unfair means which are believed and relied upon.

1.4 FURTHER DEFINITION

A fraudulent act may be an illegal, unethical, improper, or dishonest act including, but not limited to:

- a. embezzlement;
- b. misappropriation, misapplication, destruction, removal, or concealment of property;
- c. alteration or falsification of documents;
- d. false claims by students, employees, vendors, or others associated with the College;
- e. theft of any asset including, but not limited to, money, tangible property, trade secrets or intellectual property;
- f. inappropriate use of computers, including hacking and software piracy;
- g. bribery, rebate, or kickback;
- h. conflict of interest; or misrepresentation of facts.

1.5 DETERMINATION

While a fraudulent act may have criminal and/or civil law consequences, the College is not required to use a determination by a criminal justice authority to criminally prosecute as the basis for determining whether an act is fraudulent. It is the internal determination that the above criteria are present that defines an act as fraudulent under this policy.

1.6 DUTIES AND RESPONSIBILITIES

Generally, employees, students, and other persons associated with the College (collectively, members of the campus community) abide by laws, rules regulations, and policies; however, incidents of fraud may occur. Administrators at all levels of management are accountable for setting the appropriate tone of intolerance for fraudulent acts by displaying the proper attitude toward complying with laws, rules, regulations, and policies, including ethics policies. In addition, administrators should be cognizant of the risks and exposures inherent in their area of responsibility, and should establish and maintain proper internal controls which will provide for the security and accountability of the resources entrusted to them.

Any member of the campus community who has a reasonable basis for believing a fraudulent act has occurred has a responsibility to promptly notify one of the following:

- a. his or her supervisor;
- b. the appropriate administrator;
- c. Internal Audit

Employees who, in good faith, report unlawful activity are protected by the Texas Whistleblower Act against any retaliation by the College for making such a report. The reporting member of the campus community shall refrain from confrontation of the suspect, further examination of the incident, or further discussion of the incident with anyone other than the employee's supervisor or others involved in the resulting review or investigation. Persons found to be making frivolous claims under this policy will be disciplined, up to and including termination of employment or expulsion from the College.

1.7 INVESTIGATION

Supervisors and administrators at all levels of management who become aware of suspected fraudulent activity are to respond in a consistent and appropriate manner and shall report the suspected activity to the College Fraud Officer (VP Finance). With the concurrence of the Director of Audits and Compliance, the supervisor or administrator may treat the incident as an administrative issue and have a qualified individual or individuals perform an objective review as considered necessary. The Office of Audits and Compliance has the primary obligation for investigating reported incidents to the extent considered necessary for resolution. The Office of Audits and Compliance may contact other college departments to establish the necessary team to proceed with the review or investigation. The investigative team will attempt to keep source information as confidential as possible. In those instances where the investigation indicates criminal activity, the investigation shall be turned over to the appropriate law enforcement agency.

All affected departments and/or individuals shall cooperate fully with those performing a review or investigation, including the Office of Audits and Compliance, law enforcement officials, regulators, and any other parties involved. During all aspects of the review or investigation, the Constitutional rights of all persons will be observed. Suspects and others involved in the review shall be treated consistently without regard to past performance, position held, length of service, race, color, religion, sex, age, disability, national origin, or veteran status.

1.8 DISCIPLINARY ACTIONS

1.8.1 Employees found to have participated in fraudulent acts as defined by the policy will be subject to disciplinary action, up to and including termination, pursuant to personnel policies and rules. Additionally, employees suspected of perpetrating fraudulent acts may be placed on paid administrative leave during the course of the investigation. In those cases where disciplinary action is warranted, the Human Resources Office, Office of General Counsel, or other appropriate office shall be consulted prior to taking such actions. Criminal or civil actions may be taken against employees who participate in unlawful acts.

1.8.2 The employment of any employee involved in the perpetration of a fraud will ordinarily be terminated without eligibility for rehire. Actions to be taken will be determined without regard to past performance, position held, length of service, race, color, religion, sex, age, disability, national origin, or veteran status.

1.8.3 Students found to have participated in fraudulent acts as defined by this policy will be subject to disciplinary action pursuant to operating manuals. In those cases where disciplinary action is warranted, the Academic Dean, Office of Student Services, Office of General Counsel, or other appropriate office shall be consulted prior to taking such actions. Additionally, criminal or civil actions may be taken against students who participate in unlawful acts

The relationship of other individuals or entities associated with the College found to have participated in fraudulent acts as defined by this policy will be subject to review, with possible consequences including termination of the relationship. In those cases where action is warranted, the Office of General Counsel or other appropriate office shall be consulted prior to taking such actions. Additionally, criminal or civil actions may be taken against individuals or entities associated with the College who participate in unlawful acts.

1.9 REPORTING

The results of investigations conducted by the Office of Audits and Compliance shall be communicated, either orally or in writing, as determined by the Director of Audits and Compliance to the board and chancellor, or other appropriate administrator.

2. REPORTING CODE VIOLATIONS

Employees should report suspected violations of this Code, applicable laws, regulations, and government grant and contract requirements through standard management reporting channels, beginning with the immediate supervisor. Alternatively, employees may go to a higher level of management and may also report suspected violations or problems to the Director of Internal Audit. In all instances, violations of laws or regulations should be reported to the Director of Internal Audit (880-8933). Such reports may be made confidentially and/or anonymously although a greater level of information allows for a more thorough investigation. Raising such concerns is a service to the College and consistent with the State of Texas's Whistleblowers' Protection Act, will not jeopardize employment.

The Texas State University System has selected a private contractor, EthicsPoint, as a confidential means of reporting for individuals unable to use existing reporting procedures. A link is found on the TSUS web site

3. TRAINING

The System Administrative Office shall conduct, in even numbered years, training sessions for the personnel of each component institution responsible for ethics training in the various departments of such institutions. These training sessions will provide the trainees with the methods, policies and materials necessary to allow them to train each employee within their supervision or responsibility. Each component institution is responsible for training each employee each biennium. The President will notify the Chancellor upon completion of the ethics training each biennium.

4. DISTRIBUTION OF POLICY

This policy will be distributed at the beginning of each fiscal year. The Human Resources Office is responsible for the distribution. The policy may be delivered in electronic format.

5. CERTIFICATION STATEMENT

This APP has been approved by the following individuals in their official capacities and represents Lamar State College - Port Arthur policy and procedure from the date of this document until superseded.

Dr. Sam Monroe, President
Gwen Reck, Vice President Finance, College Fraud Officer
Linda McGee, Director Human Resources

POLICY: PERFORMANCE RATINGS
SCOPE: STAFF
POLICY NUMBER: 5.4
REVISED: MARCH 15, 2002

1. POLICY

This policy covers the procedures for the administration of a system for the evaluation of the performance of staff personnel holding positions at the College.

2. SCOPE AND PURPOSE

Any type of employee performance evaluation is merely a tool of management and not an end in itself. Ratings can be a positive means in assisting staff personnel in improving job performance and a rating system further affords management an opportunity to make known to staff personnel the objectives and goals of the department and of the College and what is expected of the employee toward attainment of the objectives and goals. **Staff personnel cannot be expected to meet performance standards which have not been clearly defined and explained as a part of the requirements of his/her position.**

The employee performance evaluation should be conducted on an annual basis and should not reflect personal prejudice, bias, or favoritism on the part of those conducting the ratings or reviews. The results of such evaluation procedure should be used to assist management in the decision making process of the following:

1. Determining staff personnel deserving of merit pay increases
2. Identifying staff personnel for promotion
3. Informing staff personnel of deficiencies, training needs, and improvements expected
4. Justification for disciplinary actions

Nothing in this policy or process shall be interpreted as an abdication, by the College, of its employment at will policy.

3. APPLICATION OF POLICY

These rules and procedures are applicable to all departments and divisions of the College not specifically exempted from these rules and regulations and to staff personnel for evaluation and rating techniques and for deficiency reviews.

The Human Resources Office is authorized to prepare and submit to all departments suggested guidelines and forms for developing performance evaluation systems.

4. REQUIRED PROCEDURES

Each department shall establish a system of employee performance evaluation that reflects an impartial rating of an employee's performance and his/her potential for further advancement.

Each department's employee performance evaluation system shall produce overall ratings of at least five (5) levels as follows:

0. Unsatisfactory - Performance and results achieved consistently do not meet established objectives.
1. Below Expectations - Performance and results achieved generally do not meet established objectives. Performance requires more than normal degree of supervision.
2. Meets Expectations - Performance and results generally meet the expectations for the position requirements and objectives. Performance requires normal degree of supervision.

3. Exceeds Expectations - Performance and results achieved consistently exceed expectations for the position requirements and objectives.
4. Exceptional - Performance and results achieved always exceed the standards and expectations for the position requirements and objectives.

Each staff employee shall be rated by his/her immediate supervisor whenever possible, and all ratings must be reviewed and approved by a higher level supervisor than the one who prepared the rating. It is suggested that, in all cases, the immediate supervisor doing the rating must be familiar with the performance of the staff employee during a major portion of the rating period.

Any time an employee's performance rating is **0 (unsatisfactory)** or **1 (below expectations)** the supervisor must complete the **Performance Improvement Form** (This form can be found on the HR web site or in the HR office). The supervisor will use the form to give the employee a reasonable date by which improvement must take place. In addition, if the employee has not complied with applicable college policies, procedures and work rules, and other guidelines appropriate to the position, documentation should be provided for each item.

When the **required improvement date** is reached, the supervisor will fill out the **Follow-up to the Performance Improvement Form** (This form can be found on the HR web site or in the HR office). Originals of both of these forms will be kept in the employee's personnel file in the Human Resources Office. Copies will be maintained in the department.

If during the course of the appraisal cycle, the employee performs in an outstanding manner and the supervisor wishes to recognize this performance, the supervisor will fill out the **Performance Commendation Form** (This form can be found on the HR web site or in the HR office). Original will be kept in the employee's personnel file in the Human Resources Office. Copies will be maintained in the department.

All staff personnel other than temporary appointees shall be given performance ratings upon completion of six (6) months of service following a new appointment or promotion and at least annually thereafter. Special ratings for the purpose of recognizing performance other than satisfactory may be made at any time.

5. EVALUATION AND RATING TECHNIQUES

Each department should arrange to hold periodic orientation sessions for all supervisors to train them in the techniques of a uniform and effective employee performance evaluation program. These training sessions should include presentations and discussions of such subjects as listed below:

1. Detailed explanation of the department's employee performance evaluation and rating system.
2. Instructions as to what the administration of the department expects in the way of performance standards and the requirements for disseminating this information to all staff personnel.
3. The requirements for maintaining an effective and uniform evaluation program within and among all units of the department and the desirability of the same.
4. To caution supervisory personnel who will be reviewing and evaluating the performance of subordinate employees against pitfalls of committing common rating errors such as:
 - **Central Tendency**--rating all staff personnel as average
 - **Halo Effect**--allowing one aspect of a staff employee's performance to influence the entire evaluation
 - **Overvaluation or Undervaluation**--the tendency of a rater to overvalue or undervalue a given factor, and

- **Miscellaneous Biases**--race, sex, nationality, religion, personality conflicts, etc.
5. Rating factors are the criteria by which staff personnel are evaluated. Some of the common rating factors and their descriptions are listed below; however, there are other factors that could be considered.
- **Quality of work**--degree of accuracy, completeness, and neatness of duties performed by employee
 - **Productivity**Buse of available work time, plans and prioritizes work, sets and accomplishes goals, completes assignments on schedule
 - **Knowledge of job**Bduties and requirements of position, methods, practices and equipment; experience, education and specialized training; maintains current knowledge about changes in policy and procedures
 - **Adaptability**Bability to learn quickly, to adapt to changes in job assignments, methods, personnel, or surroundings
 - **Dependability**Breliability in performing work assignments and carrying out instructions; degree of supervision required and willingness to take responsibility; accountability
 - **Initiative and resourcefulness**B-ability to be self starter, to offer suggestions, to anticipate needs and to seek additional tasks; ability to contribute, develop and/or carry out new ideas or methods
 - **Judgments**Bability to evaluate situation and make sound decisions; ability to identify, solve and prevent problems; works in a safe manner, preventing accidents, injuries and theft
 - **Campus Citizen**--relationship with others, the ability to work cooperatively with fellow employees
 - **Attendance and Punctuality**--How often is employee late or tardy for work? Consider patterns of sick leave, prior approval for vacation and prompt notice of absence due to illness; consider arrival times, observance of time limits for breaks and lunches

6. CORRECTIVE REVIEW POLICY

A policy of corrective review is an important factor in avoiding problems that may occur during an employee's tenure with the College. The following procedures will be used by department heads, directors, and supervisors, with reasonable efforts being made to resolve personnel problems, prior to the dismissal of an employee, unless, in the College=s judgment, the best interests of the College require dismissal.

1. When a personnel problem arises, it must be given immediate attention by the appropriate supervisor.
2. The employee/employees affected by the problem will be required to meet with their immediate supervisor for a corrective review concerning the problem.
3. The review must be constructive, giving the employee reasonable opportunity to correct the situation.
4. The employee, at this time, will be informed of the indicated problem area concerning his/her job performance and will be instructed by the supervisor concerning corrective measures to be taken.

5. The corrective review will be documented on the **Performance Improvement Form**. The documentation will include a description of problems, a date for improvement and specific actions for correcting the situation. Documentation will also include what action steps the supervisor will take to help the employee correct the situation. The review will then be signed by the supervisor and the employee. The review will be made part of the personnel record.
6. If additional meetings are required to resolve the same situation, the employee may be placed on probation, as determined by the department head with the approval of the appropriate Dean or Vice President. The employee is advised of the probation period, the cause of such probation, the corrective procedures, and that this will be a part of his/her personnel record.
7. At the end of the probation period, the employee and supervisor will review the progress made. When sufficient improvement is noted, the probation can be removed at the discretion of the supervisor. The conclusions will be written for the personnel record on a specific memorandum. If the employee fails to respond satisfactorily to the conditions of probation, he or she may be dismissed. (Section 5.3-Disciplinary Actions -Staff)

POLICY: PERFORMANCE RATINGS
SCOPE: FACULTY
POLICY NUMBER: 5.5
REVISED: MARCH 15, 2002

Faculty members are evaluated annually by their Department Chairs relating to various professional duties and activities including classroom instruction, participation in department and College affairs, professional development and service, and community service.

The Annual Faculty Report (F2.08) may be used for faculty self evaluation, and may be used by the Deans and Vice President for Academic Affairs to support recommendations concerning promotion, tenure, and salary administration. Faculty members receive a copy of this evaluation report after the Dean and Vice President have completed their reviews and have the right to request a conference concerning departmental evaluations and to appeal such evaluations.

Divisions are encouraged to use student evaluations of faculty as an aid to the faculty in improving instruction. Such evaluations, however, are not a part of consideration for promotion or tenure.

POLICY: DISCIPLINE
SCOPE: STAFF
POLICY NUMBER: 5.6
REVISED: MARCH 8, 2004

1. SCOPE AND PURPOSE

In order to establish a sound system of Personnel Administration for Lamar State College - Port Arthur, it is necessary that:

- Administrative and supervisory personnel have the responsibility and authority to resolve employee problems as they arise.
- Similar offenses by staff personnel are handled in a uniform manner in all departments and administrative subdivisions of the College.
- Staff personnel have a sense of security in their employment with the knowledge that capricious and arbitrary disciplinary action will not be taken against them.

The rules and procedures established in this section apply to all staff personnel covered by these rules and regulations.

2. APPLICATION OF POLICY

This section includes the rules and procedures applicable to the staff personnel of the College in regard to disciplinary actions, grievance procedures, appeals, and reviews.

- Each dean, department head, director, or other administrative head of the subdivisions of the College shall insure that all staff personnel covered by these rules are made aware of the provisions of these rules and shall inform all staff personnel under his/her administrative jurisdiction that they have the right to express their grievances or submit an appeal without fear or coercion, discrimination, or reprisal by any subordinate, administrator, or supervisor.
- Only the President has the authority to discharge an employee.

3. DISCIPLINARY ACTION

In order that each supervisor and staff employee can be able to perform his/her respective duties efficiently and effectively, it is necessary that departmental administrators establish clearly defined departmental objectives, work performance standards, standards of conduct, and other departmental policies which are applicable in given work situations.

To maintain established standards and to insure that all staff personnel adhere to reasonable rules of conduct, it is necessary that each department establish rules and procedures which will insure timely and equitable disposition of actions determined to be necessary in dealing effectively with employee deficiencies or breach of good conduct.

Disciplinary actions and the imposition of reasonable penalties for specific offenses should be viewed by a subordinate as constructive procedures in reaching established standards rather than as punishment to the staff employee.

The following are examples of recommended but not required disciplinary actions. It is not required that disciplinary action must occur in order listed.

1. **Oral Warning** - This is the least severe disciplinary action. The employee should clearly understand the gravity of the action and that the warning is disciplinary in nature. When presenting a corrective talk the supervisor should point out the error/problem(s), explain how to correct it, and come to an understanding with the employee about what is expected in the future. The Staff Verbal Warning Form will be completed and kept in the supervisor=s file.
2. **Written Warning** - When an oral warning fails to achieve the desired improvement in performance or behavior or when in the supervisor=s sole judgment the nature of the offense makes its use appropriate, the supervisor may issue a written warning. A Staff Written Warning

Form is used to issue a written warning. The Human Resources Department should be contacted for assistance in preparing a written warning and the Director of Human Resources may be present if desired by the supervisor when the warning is presented to the employee. The written warning should be forewarning of potential actions; be clear, focused and complete; be based upon facts that have been fully investigated; be consistent and applied equally to all; and it must not violate an employee's civil rights. The completed Staff Written Warning Form will be placed in the employee's personnel file for future reference.

3. **Demotion** - When in the sole judgment of the supervisor demotion is the best corrective method to remedy poor performance or behavior, this may be implemented with the approval of the Director of Human Resources. When an employee is demoted to a position of decreased responsibility or complexity of duties requiring a change of title to one having a lower salary range, the employee's salary will be adjusted to an appropriate level within the new salary range as agreed upon by the Department Head concerned and the Director of Human Resources. A Personnel Action Request Form (F3.2) must be prepared in consultation with the Director of Human Resources. The employee will be advised of the action in a meeting with supervisor which may include the Director of Human Resources.
4. **Suspension Without Pay** - When any one or a combination of the above possible actions have failed to achieve the supervisor's desired results or when in the judgment of the supervisor the nature of the offense makes its use appropriate, the supervisor may suspend an employee without pay. The action must have the approval of the Director of Human Resources. A Personnel Action Request Form (F3.2) and a Staff Notice of Disciplinary Suspension Form must be prepared in consultation with the Director of Human Resources. The employee will be informed of the suspension in a meeting with the supervisor which should include the Director of Human Resources. The suspension period must be in accordance with the Fair Labor Standards Act (FLSA). FLSA overtime exempt employees must be suspended in weekly increments except for infractions of significant safety rules as defined by the Department of Labor. The Personnel Action Request Form (F3.2) will be forwarded to the Human Resources Office. The Staff Notice of Disciplinary Suspension will be forwarded to the Human Resources Office and be placed in the personnel file.
5. **Discharge** - This action may be the result of one serious act of misconduct or insubordination, or as the result of an accumulation of minor offenses, or failure to satisfactorily perform job duties. All discharges must have the prior approval of the President and the Director of Human Resources. When an employee is suspected of committing a serious act of misconduct, which in the judgment of the supervisor requires immediate action, and it is not possible to obtain the prior approval, the supervisor may suspend or discharge the employee pending the receipt of the necessary approval. The employee will be informed of the discharge in a meeting with the supervisor and the Director of Human Resources. A Personnel Action Request Form (F3.2) will be forwarded to the Human Resources Office.

4. **DOCUMENTATION**

All staff employee disciplinary actions must be documented. The appropriate form must be used to document the reason or reasons for the disciplinary action.

5. **REGENTS RULES**

The provisions of this policy are subject to the Board of Regents's Rules. Those portions of Chapter V of the Regents' Rules specifically related to employment and termination are incorporated by reference into this policy. In case of any conflict between this policy and any provisions of the Rules, the Rules shall prevail.

POLICY: **DISCIPLINE**
SCOPE: **FACULTY**
POLICY NUMBER: **5.7**
REVISED: **DECEMBER 12, 2003**

The Academic community cannot tolerate actions by its own members that hinder or make less effective the carrying out of its mission. The demands of academic responsibility and professionalism apply to all those who teach at Lamar State College - Port Arthur, tenured or non-tenured, full-time or part-time.

Faculty who violate any Lamar State College - Port Arthur policy are subject to the faculty disciplinary process.

The concept of progressive discipline acknowledges that a faculty member may be guilty of an employment offense or misconduct that, while serious, does not necessarily justify immediate dismissal. Faculty member=s activities that fall outside the scope of employment shall constitute misconduct if such activities adversely affect the interests of Lamar State College - Port Arthur.

DISCIPLINE OPTIONS

Disciplinary actions imposed on a faculty member may include both punitive and corrective actions. These actions may extend from mild to severe and will be administered based upon the seriousness, frequency and/or flagrant nature of the infraction. When appropriate, progressive discipline will be employed as follows:

- First incident - oral reprimand
- Second incident - written reprimand
- Third incident - probation
- Fourth incident - dismissal

Some violations may be of such a nature that progressive discipline is not appropriate. In those instances, administration may choose to employ sanctions not of a progressive nature. Written documentation of all/any disciplinary action other than an oral reprimand will be placed in the personnel file.

The Vice President for Academic Affairs and the Director of Human Resources shall review all disciplinary action to ensure EEO compliance. The review will include a comparison of disciplinary actions of other similarly situated circumstances.

POLICY: GRIEVANCE
SCOPE: STAFF
POLICY NUMBER: 5.8
REVISED: MARCH 15, 2002; DECEMBER, 2005

1. POLICY

Every employee of Lamar State College - Port Arthur is entitled to present grievances concerning such individual's wages, hours of work, or conditions of work individually or through a representative that does not claim the right to strike. (The Texas State University System Rules and Regulations, May 1999). Employees having work-related problems are encouraged to discuss the problem with the immediate supervisor. If the problem cannot be resolved through this informal process, the employee may file a formal grievance.

Except where otherwise stated in this grievance procedure, employees may represent themselves or be represented by a fellow employee or other representative, with the exception of an attorney, while exercising the rights provided in this grievance procedure.

All meetings and investigations related to grievance reviews shall be conducted during the staff employee's regular working hours insofar as possible.

The College will guarantee and insure that staff personnel subject to these rules shall be afforded fair, equitable, and expeditious hearing of matters of grievance without fear of coercion, discrimination, or reprisal because of exercising the right of request for redress from grievance.

2. PROCEDURES

The grievance procedures for staff personnel covered by these rules are as follows:

1. The regularly established administrative channels shall be the route of all matters of grievance.
2. A staff employee shall at first present in **writing** any matter of grievance to his/her immediate supervisor. This should be done within three (3) working days from the beginning of the grievance. Upon receipt of the grievance as submitted by the employee, the immediate supervisor shall consider all of the facts of the case and he should report his decision in the matter in writing to the employee within two (2) working days after receipt of the grievance.
3. If the matter is not satisfactorily resolved in the eyes of the grievant, he/she may continue to have the grievance heard and adjudicated by each level of supervision in the regular administrative channel until the level of the Dean or Vice President is reached. At each level above the first supervisor, the request for grievance hearing must be made by the grievant and should be submitted in writing within three (3) working days from the delivery of the decision of the lower supervisor. At each level of hearing, the supervisor will review all the facts of the case and the decisions rendered by the lower supervisors, and then he/she should render a decision in writing to the grievant within three (3) working days after receipt of the grievance.
4. If the matter continues to be unresolved in the eyes of the grievant, he/she may then submit the grievance in writing to the President. This shall be done within five (5) working days after receipt of the decision of the Dean or Vice President.
5. The President may decide to appoint a Grievance Review Committee to help review the grievance or he may elect to review the grievance personally.
6. The President or Committee shall conduct an investigation of all the events leading to the grievance, review all decisions rendered by lower supervisors, and render a decision in writing as soon as possible after the investigation is complete. The decision of the President shall be final in all cases of grievance.

At any step or level of the grievance procedure, the Human Resources Office may be requested by the grievant or the supervisor to serve as consultant to the grievance hearing. In such cases, the

Human Resources Office shall serve in the capacity of an information-gathering and advisory member only, and shall not have the power of making binding decisions.

A complaint or grievance in which a staff member alleges that disciplinary or dismissal action has been taken without adequate cause, and the staff member alleges that illegal discrimination has occurred on the basis of race, color, religion, sex, age, national origin, or non-job related mental or physical handicap, should be referred and discussed with the Human Resources Office.

3. GRIEVANCE REVIEW COMMITTEE

1. The Committee will consist of five staff employees appointed by the President. The Committee should include professional as well as classified staff. All members must be present to conduct any business.
2. The Committee should meet within ten days after the notification of their appointment by the President. The committee should meet prior to the hearing to review the process and select a chairperson to conduct the hearing.
3. The Chairperson shall be responsible for setting the date and time for the Hearing, and notifying Committee members, the grievant, and the person against whom the grievance has been filed. The Chairperson may grant one postponement at the written request of one of the parties. A postponement should not exceed one week of the original Hearing date.
4. The Committee Chairperson should receive documents pertinent to the Hearing at least two (2) days prior to the Hearing. Required documents include:
 - a. The employee's original grievance
 - b. The supervisor's decision in the matter
 - c. Any subsequent decisions in the matter
 - d. A list of witnesses from both parties
 - e. Any relevant documentation either party wishes to provide (The Chairperson has the authority to exclude irrelevant, immaterial, or unduly repetitious documents.)
5. The Hearing may be tape recorded in lieu of a hand written record.
6. The following persons may be present during the Hearing. Witnesses will not be allowed in the Hearing room except to testify.
 - a. The grievant
 - b. The grievant's representative, with the exception of an attorney
 - c. The department representative(s) against whom the grievance has been filed (a spokesperson must be designated if more than one representative appears)
 - d. Committee members
 - e. The Director of Human Resources

4. The Grievance Hearing

1. The Grievance Hearing shall be conducted by the Committee Chairperson.
2. The order of the Hearing shall be:
 - a. The Chairperson shall open with a statement that includes the purpose of the Hearing and a warning to all present to maintain the confidentiality of the Hearing.
 - b. The Chairperson shall allow the grievant to make an opening statement. The grievant will then respond to questions from committee members as well as the individual against whom the grievance was filed.

- c. The Chairperson shall allow the individual against whom the grievance was filed to make an opening statement. The individual will then respond to questions from the committee members as well as the grievant.
- d. The Chairperson shall allow the grievant to call any witnesses. The witness will then respond to questions from committee members and the individual against whom the grievance was filed. Witnesses are only allowed in the Hearing to present testimony and answer questions.
- e. The Chairperson shall allow the person against whom the grievance was filed to call any witnesses. The witnesses will then respond to questions from the committee members and the grievant.
- f. The committee may wish to call witnesses not called by either party. Committee members and both parties may question the witnesses.
- g. The Chairperson shall allow the grievant and then the individual against whom the grievance was filed to make concluding statements.
- h. The Chairperson shall ask that everyone clear the room except committee members. The committee will submit a written finding of facts and propose a recommendation to the President within three (3) working days. The recommendations must be based on a majority vote of the committee members.
- i. The President will make a final decision and submit it to the grievant within three (3) working days.

POLICY: **TERMINATIONS**
SCOPE: **STAFF**
POLICY NUMBER: **5.9**
REVISED: **MARCH 5, 2002; DECEMBER 2005**

1. POLICY

The President of Lamar State College – Port Arthur shall have the authority to terminate at any time the employment of any classified staff employee and any other non-faculty personnel with the exception of administrative officers subject to the review of the Board of Regents.

Employees, including both faculty and staff, shall be subject to discipline and/or dismissal for violating college policy relating to electronic network facilities such as local area networks and the Internet. Nothing herein shall be construed in derogation of the Board's employment-at-will policy.

Employees may be terminated without notice within the confines of other policies established in the Administrative Policies and Procedures Manual.

The minimum standards of individual conduct required by the penal statutes of Texas or the United States are both expected and required of every employee of Lamar State College - Port Arthur. Any employee who violates the minimum standards of conduct required by any penal statute of Texas or the United States is subject to discipline or dismissal as an employee regardless of whether any action is taken against the employee by civil authorities on account of such violation.

If action for dismissal of an employee is taken, the appropriate administrative officer shall proceed with the action in the same manner as would be the case of a violation by an employee of any other provision of the Administrative Policies and Procedures Manual.

Terminated employees may not use campus facilities such as the computer labs, gymnasium, or library. Security personnel will take immediate action to remove terminated employees without authorization to use campus facilities. Students who have been terminated as an employee may continue to use facilities as required for the course(s) in which they are currently enrolled.

It is the responsibility of each department to notify the Human Resources Office as soon as possible when an employee terminates for any reason. The department should submit an F3.2 through normal channels along with any appropriate documentation such as letters of resignation or termination

2. RESIGNATIONS

2.1 Faculty

A faculty member should not resign later than May 15th or thirty (30) days after receiving notification of the terms of continued employment for the following year, whichever date occurs later. It is recognized that emergencies will occur. In such an emergency, the faculty member may ask the President of the College through normal academic channels to waive this requirement; but, the faculty member should conform to the President's decision.

2.2 Staff

A staff member is normally expected to give two weeks advance notice of resignation from employment. Notice should be in writing and should contain the reasons for resignation. Any employee who is absent from work without authorized leave for three (3) consecutive workdays shall be deemed to have abandoned his/her position and to have voluntarily resigned from employment. Should an employee seek to return to work after such unauthorized leave, the employee must provide satisfactory proof that the failure to request authorized leave was justifiable and excusable. An employee providing such satisfactory proof may be returned to their original position at the discretion of management. Other disciplinary action is optional.

3. REDUCTION IN FORCE

A reduction in force is defined as a layoff of a segment of the work force due to a lack of work, reduction in funding, or reorganization. It is an involuntary termination of employment not involving delinquency or misconduct.

The President of the College may implement a reduction in force in order to meet operating expenses and maintain sound reserves without diminishing capital or generating unwise or impermissible indebtedness. Prior to the implementation, The President shall consult with the Vice Presidents and other Administrator of the President's choice. The consultation shall include a discussion of:

1. anticipated income and expenditures;
2. retrenchment measures which have been taken;
3. reasonable alternatives to reduction in force; and
4. any other matter the President deems appropriate.

Policy:

1. Regular, full-time employees will be given preference for retention over probationary, part-time, or temporary employees.
2. Decision is to be based on the operation of the job function, not on the performance attributes or seniority of the incumbent.
3. Employees who are laid off as a result of a reduction in force will be given priority consideration for vacant positions for which they qualify.

Procedure:

1. The President will designate the departments or functional areas of reductions.
2. Whenever possible staff members will receive notification of change in employment status not later than thirty (30) days prior to the date of the actual change.
3. Staff members who have been laid off will receive a lump sum payment for all accrued vacation leave.
4. Sick leave balance at the time of layoff will be restored if the employee is rehired by a State agency within twelve (12) months.
5. Current group insurance coverage may be retained for eighteen (18) months under the Consolidated Omnibus Budget Reconciliation Act (COBRA). The employee must pay the total monthly premium for the coverage. Life insurance conversion options are also available.

4. EXIT INTERVIEWS

It is important that an exit interview be conducted with any benefits-eligible separating employee by the Human Resources Office to discuss the following:

5. COMPENSATORY TIME PAY (Comp Time)

Non-exempt employees are entitled to be paid a lump sum payment for any accrued FLSA Compensatory time.

Non-exempt employees are not entitled to be paid for any accrued State Compensatory time.

6. INSURANCE

Insurance coverage ends on the last day of the month in which employment ends. Health and dental coverage may be continued for any participating employee and/or dependents for up to 18 months under the Consolidated Omnibus Budget Reconciliation Act (COBRA). To continue coverage, the employee must return the COBRA Election form within 60 days of the "Date of the Event."

7. SICK LEAVE POOL

Separating employees are encouraged to contribute to the Sick Leave Pool if eligible.

8. RETIREMENT OPTIONS

Employees on the Teacher Retirement System may elect to leave their money in place where it will continue to draw interest or request a refund. Employees requesting a refund may elect to receive the account balance less 20% for income tax or place the balance in an eligible retirement plan.

When an employee terminates who is a participant in the Optional Retirement Program (ORP), the employee may elect to surrender the ORP account if further employment with a State-supported institution of higher education is not contemplated. For a vested individual (one year plus one day of participation), the entire benefits provided by the contract are the sole non-forfeitable possession of the individual. If the individual has not met the vesting requirements, the carrier must return the state contribution to Lamar State College - Port Arthur with the balance of the annuity value returnable to the individual.

9. FINAL PAYCHECK

The final paycheck may be picked up (or direct deposited) on the next regular pay day following termination.

10. TRAVEL REFUNDS

Departing employees are advised to check with the Finance Office to determine the status of outstanding travel reimbursements. If necessary, a forwarding address should be provided, the Business Office is responsible for distribution of reimbursements.

11. SIGN OUT PROCEDURES

Documents to be returned to Human Resources

- Employee ID Card
- Medical Insurance Card
- Credit Card
- Parking Permit
- Keys

To be received by the Supervisor

- Resignation Letter
- College Property

Departments are required to remind exiting employees of the exit interview process.

POLICY: TERMINATIONS
SCOPE: ADMINISTRATIVE OFFICERS
POLICY NUMBER: 5.10
REVISED: DECEMBER 2005

1. POLICY

The President or Chancellor may terminate the employment of an administrative officer of the College when in their judgment the interest of the System or of the College requires termination. An Administrative Officer shall not have a right to a hearing unless the officer makes a *prima facie* showing that the decision to terminate violates rights guaranteed by the laws or Constitution of the State of Texas or of the United States and requests an administrative hearing to review the allegations. In such case the administrative officer shall be afforded an opportunity to present allegations before a hearing committee consisting of three impartial administrative officers of the College appointed by the President. Such allegations shall be heard under the same procedures as in the case of dismissal of staff for cause, with the following exceptions:

- 1.1 The burden of proof is upon the affected administrative officer to establish at such hearing that the decision in question constitutes violation of a right guaranteed by the laws or Constitution of the State of Texas or of the United States.
 - 1.2 The President of the College need not state the reasons for the questioned decision nor offer evidence in support thereof unless the affected administrative officer presents a *prima facie* case in support of such allegations. In such case, the hearing committee shall determine whether the president has no other reason for his decision.
 - 1.3 The hearing committee will make written findings on the material facts and a recommendation, which findings and recommendation shall be forwarded to the President and to the affected administrative officer. The administrative officer may appeal to the President and ultimately to the Board of Regents in accordance with the terms and procedures as in the case of dismissal of faculty for cause.
2. If the administrative officer has tenure at the College by virtue of holding a past faculty position or otherwise, termination as a member of the tenured faculty shall be only for good cause shown, and the official shall be given a hearing if terminated from tenured faculty status.

POLICY: USE OF STATE PROPERTY
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.11
REVISED: MARCH 15, 2002; DECEMBER 2005

1. POLICY

State property may be used only for official state purposes and should not be used for personal purposes. This includes the use of state-owned or state-leased vehicles, which may be used only for official state business. The use of such vehicles to commute to and from work is acceptable if it is approved by the administrative head of an agency. The names and job titles of these employees and the reasons for authorization must be included in the annual report that the agency is required to submit under Texas Government Code, Section 2101.0115.

2. OFFICE EQUIPMENT

The use of state property including telephones and office equipment should be restricted to official business. It is expected that any personal business conducted over the telephone will be kept to a minimum. Excessive personal phone calls or use of photocopiers, typewriters, etc. for personal reasons may lead to restrictions or disciplinary actions. In no case will personal long distance phone calls be charged to Lamar accounts.

3. TOOLS/EQUIPMENT

Tools or equipment used in official duties shall not be used for personal reasons. Any personal mail sent through the College Post Office must be paid for by the employee. Removing state property from the campus for personal use is expressly forbidden. Any employee wishing to take Lamar property home to work on official business must receive permission from his/her supervisor to do so. Failure to comply with these policies is cause for disciplinary action up to, and including, discharge.

4. PROCEDURE

Any time state property is taken off campus; a form must be completed and approved by the Property Manager and the department head. Forms are available from physical plant, the computer center, and the mail room.

POLICY: SOCIAL EVENTS WITH ALCOHOL
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.12
REVISED: MARCH 15, 2002

1. POLICY

It is the policy of Lamar State College - Port Arthur that use of alcoholic beverages during work time is prohibited. All social events where alcohol beverages are served are subject to the following regulations.

2. FACILITY RESERVATIONS

Use of college facilities will be granted only to groups or organizations which have the approval of the Vice President of Student Services.

A "Request for Facilities" form must be signed by the organization president and the College advisor for the organization; a reservation form must be signed by an appropriate official of the group.

Reservations for use of the Student Center, bandstand, and pavilion facilities are made in the Student Service Office ext. 7157. Requests for use of other facilities, such as the Carl A. Parker Multipurpose Center, the Vuylsteke Home and the Performing Arts Center, should be addressed to the administrative office in charge of that facility.

3. STIPULATIONS REGARDING TIME AND PLACE

Alcoholic beverages may not be served until after 5 p.m. Monday through Friday without explicit authorization. Alcohol may be served in authorized facilities Monday - Thursday, 5 p.m. until midnight; Friday, 5 p.m. until 2 a.m.; Saturday, 10 a.m. until 2 a.m.; Sunday, noon until midnight. Ordinarily facilities are unavailable during holiday periods. Beverage and bartender service will be discontinued thirty (30) minutes prior to the scheduled ending time of an event.

No alcohol may be possessed, served, or consumed in or near an area used for classroom instruction while classes are being held in such an area.

Alcoholic beverages may be served or consumed, with prior approval, in the following approved areas: Student Center 4th Floor, Gates Library, the Carl A. Parker Multipurpose Center, the Vuylsteke Home, and the Performing Arts Center. When approved by the President, alcoholic beverages may be permitted in certain areas of other facilities.

Alcoholic beverages are restricted to the specific area designated on the reservation form.

4. FOOD SERVICE

Food should be served at all events when alcoholic beverages are served. Arrangements for food should be made in advance. When alcoholic beverages are served, each group/organization is responsible for providing the alcoholic beverages in the advance of the event. Time and place of delivery and pick-up will be designated by the Vice President of Student Services or other administrative officer at the time the reservation is made. Alcoholic beverages must be delivered in bulk form by a representative of the sponsoring organization. Individual members or guests may not individually bring alcoholic beverages to a social function.

An admission fee cannot be charged at an event where alcohol is served unless an alcohol sales license has been provided for and permission has been given by appropriate College officials.

5. RESPONSIBILITIES

The president of the organization is responsible for the delivery/pick-up of the bulk quantities of alcohol to the building coordinator or his/her designate.

Signatures indicate full acceptance of responsibility for the organization's use of the facilities and compliance with state regulations regarding the consumption and distribution of alcohol.

A minimum of two (2) police officers are required at all dances/mixer-type events where alcohol is served or where the building coordinator, advisor, or Vice President of Student Services deems necessary.

All adjustments to these regulations shall be communicated in writing to the advisor and/or officers of the sponsoring group or organization and have the prior approval of the Vice President of Student Services.

The group or organization reserving a facility is responsible for any charges for damages and clean-up which result from an organization's function.

Any violation of these policies will be referred to the Vice President of Student Services for disciplinary action. Violations may result in denial of the use of facilities and/or disciplinary action.

6. LEGAL CONSIDERATIONS

Appropriated funds may not be spent on alcoholic beverages or to reimburse a travel expense that was incurred for an alcoholic beverage.

When alcoholic beverages are served, a fee may not be charged for the event except when provided for by license.

All state regulations and statutes regarding possession, serving, and/or consumption of alcoholic beverages and the "Lamar State College - Port Arthur Policy Governing On-Campus Social Events", Lamar State College - Port Arthur Student Handbook will be strictly enforced. Violators of these regulations/statutes/policies are subject to disciplinary action by the college and by civil authorities.

The Vice President of Student Services or his or her designate has the prerogative of making adjustments in these policies in the best interest of the College.

POLICY: DRUG AND ALCOHOL ABUSE
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.13
REVISED: MARCH 15, 2002

ADMINISTRATORS SHOULD EXERCISE EXTREME CAUTION IN ALL MATTERS RELATING TO THIS POLICY, ASSURING THAT PROCEDURES ARE CAREFULLY FOLLOWED AND THAT SUBSTANTIAL EVIDENCE FROM RELIABLE SOURCES SUPPORTS A DECISION TO CONFRONT A STUDENT OR EMPLOYEE.

1. PURPOSE

Based on its commitment to assure the safety and health of its students and employees, Lamar State College - Port Arthur seeks to maintain a work and learning environments 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.

This policy is based on the following objectives:

1. To maintain a safe and healthy environment for all 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.
8. 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 Drug or Controlled Substance:** any substance, including alcohol, capable of altering an individual's mood, perception, pain level or judgment.
- 2.2 Prescribed drug:** 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.
- 2.2 Illicit drug or chemical substance:** (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.
- 2.3 Controlled substance:** means a controlled substance in schedules I through 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.

- 2.4 **Alcohol:** 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."
- 2.5 **Alcohol abuse:** 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.
- 2.6 **Conviction:** a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charge with the responsibility to determine violations of the Federal or State criminal drug statutes. (See 9.5 for time limitations on reporting such convictions.)
- 2.7 **Cause for reasonable suspicion:** established by: (1) observation; (2) action/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.
- 2.8 **Criminal drug statute:** a criminal statute involving manufacture, distribution, dispensation, use, or possession of any controlled substance.
- 2.9 **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.
- 2.10 **Workplace:** means any office, building, classroom, or property (including parking lots) owned or operated by the College, or any other site at which the employee is to perform work.
- 2.11 **Employee:** any faculty, staff or student receiving remuneration for services rendered.
- 2.12 **Possess:** means to be contained either on an employee's person or in an employee's vehicle, tools, or areas entrusted to the employee.
- 2.13 **Impaired:** means under the influence of an illegal drug or alcohol such that the employee is unable to perform his/her assigned tasks properly.

3. POLICY

3.1 STANDARDS OF CONDUCT

- 1. The unlawful manufacture, distribution, possession or use of illicit drugs or alcohol is strictly prohibited.
- 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 above.
- 3. The College shall conduct a biennial review of its drug and alcohol abuse prevention program. It shall determine and put in report format:
 - a. the effectiveness of the program,
 - b. the consistency of the enforcement of sanctions imposed pursuant to the program.

It shall also evaluate whether any changes are needed and shall implement any such changes.

4. The College shall have available for review by the Secretary of Education, or designee, and the general public, if requested, copies of all documents distributed to students and employee under the drug and alcohol abuse prevention program and copies of the institution's biennial review.

4. DRUG FREE AWARENESS PROGRAM

The College shall distribute annually to each employee and student, if applicable, information pertaining to:

1. Standards of conduct that prohibit the unlawful possession, use, and distribution of illicit drugs and alcohol by students and employees on the College's property or as part of any College activity.
2. A description of the applicable legal sanctions under local, state, or federal law for the unlawful possession or distribution of illicit drugs or alcohol.
3. A description of the health risks associated with the use of illicit drugs and the abuse of alcohol.
4. A description of any drug or alcohol counseling, treatment, or rehabilitation or re-entry programs that are available to students or employees.
5. A clear statement that the College, consistent with local, state, or federal law, will impose sanctions against a student or employee who violates the standards of conduct. The statement must describe the possible sanctions, which may include completion of an appropriate rehabilitation program, expulsion from school, termination of employment, or referral to the authorities for prosecution.
6. A description of the institution's drug/alcohol abuse prevention and intervention program, including alternative support, education and re-entry programs for students who are suspended as a result of violating standards required by these minimum requirements.
7. The College shall certify the availability of a drug abuse prevention program for officers, employees and students of the institution, as required under Title IV of the Higher Education Amendments of 1986 (P.L. 99-498).

5. SUSPICION OF USAGE

If a supervisor reasonably suspects that usage of a controlled substance or of alcohol has affected an employee's job performance, the supervisor shall immediately notify the appropriate department head, or other designated administrative official, and upon direction, the supervisor or other designated administrative official shall discuss with the employee the suspected drug-related problems. The employee should be advised of any available drug counseling, rehabilitation, or employee assistance programs, and the terms of any applicable period of probation. All such meetings between the employee and the supervisor or other designated administrative official to address the suspected drug-related problem and/or its resolution shall be documented in a memorandum to the record and filed in the employee's personnel file.

Should such discussion and/or participation in any available drug counseling, rehabilitation, or employee assistance program fail to resolve the suspected drug-related problems, or should the employee fail to meet the term of any applicable probation period, the employee may be subject to termination, or a chemical screening may be required as provided in 7. **PROCEDURE FOR TESTING (CHEMICAL SCREENING)**.

6. RULES FOR TESTING

- 6.1** Employees in a sensitive position may be tested for the use of illicit drugs. "Employee in a sensitive position" means an employee who has been granted access to classified information or employees in other positions determined by appropriate administrative personnel to involve national security, health or safety concerns, or functions requiring a high degree of trust and confidence.

7. PROCEDURE FOR TESTING (CHEMICAL SCREENING)

- 7.1** The decision to require a chemical screening must be reviewed with legal counsel prior to the screening.
- 7.2** Prior to the administration of chemical screening, the appropriate administrative or supervisory personnel must explain the chemical screening procedures to the employee and then accompany the employee to a hospital or clinic for the taking of a specimen for screening purposes.
- 7.3** Before the specimen is taken, the employee should be asked to sign a consent form agreeing to the taking of a specimen for testing purposes. The signed form will be required by the hospital or clinic. The employee will be asked to list any medications taken. There will be a reasonable opportunity to rebut or explain a positive test result, including an independent retest of the sample.
- 7.4** The expense of the test, and any retest, shall be borne by the College. The testing procedure will be kept confidential, with the results being reported to the employee and the appropriate senior-level administrator as soon as they are available.

8. REGULATIONS SPECIFICALLY RELATED TO EMPLOYEES

- 8.1** A copy of this policy shall be provided to each employee who is or who will be engaged in the performance of a federal grant or contract, and a record shall be kept of the distribution.
- 8.2** Any employee whose off-duty use of drugs or other controlled substances results in absenteeism, tardiness, impairment or work performance, or is the cause of workplace accidents, will be referred to an assistance program and may be subject to discharge if he or she rejects participation in the program.
- 8.3** Employees in sensitive positions whose work-related performance gives cause for suspicion of use or possession of a controlled substance may, at the discretion of appropriate authorities be subjected to testing for the substance in accordance with the sections in this policy related to testing and chemical screening. A refusal to submit to a test, combined with a reasonable suspicion of usage, may be a sufficient basis for termination.
- 8.4** Any disciplinary action shall be governed by College policies on discipline and dismissal and academic freedom, responsibility and tenure. Sanctions may include a period of probation for an employee. A record of the action will be placed in the employee's personnel file.
- 8.5** As a condition of employment, employees on government grants or contracts must abide by the required notification statement and must report any criminal drug statute conviction for a violation occurring in the workplace or on College business to their employer no later than five days after such conviction. The employer, in turn, must so notify the contracting federal agency within 10 days after receiving notice from an employee or otherwise receiving actual notice of such conviction, and within 30 days must impose sanctions on the employee, up to and including termination, or requiring the employee to satisfactorily participate in an approved drug abuse assistance or rehabilitation program.

9. AUTHORITY OF PRESIDENT

The President of Lamar State College - Port Arthur is authorized to approve any changes to this policy to bring the College into full compliance with instructions of the Board of Regents, applicable legislation, or guidelines promulgated by local, state, or federal governmental bodies.

POLICY: SMOKE-FREE WORKPLACE
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.14
REVISED: MARCH 15, 2002; DECEMBER 2005

1. POLICY

Lamar State College - Port Arthur recognizes its commitment to the emotional and physical well-being of its students, faculty, and staff. There is increasing concern, interest, and anxiety about the effects of secondary tobacco smoke on individuals exposed to it and the dangers associated with tobacco smoking. Lamar State College - Port Arthur acknowledges the seriousness of this problem and recognizes its obligation to promote public health on this campus by protecting its students, faculty, and staff from hazardous conditions which are within the College's ability to regulate.

2. REGULATIONS

The following regulations have been adopted by Lamar State College - Port Arthur.

- 2.1** ALL campus buildings are designated "smoke free." Included in this designation are all instructional facilities; faculty, staff, and administrative offices; and student services areas.
- 2.2** The use of smokeless tobacco, including snuff and chewing tobacco, is prohibited on campus.
- 2.3** The sale of tobacco products on campus is prohibited.
- 2.4** Smoking is prohibited in those campus-owned vehicles that are available for general use.
- 2.5** As used in this policy, the term "smoking" shall include all of the following:
 - 1. Carrying or holding a lighted pipe, cigar, cigarette, or any other lighted smoking equipment or device;
 - 2. Lighting a pipe, cigar, cigarette, or any other smoking equipment or device;
 - 3. Emitting or exhaling the smoke of a pipe, cigar, cigarette, or any other smoking equipment or device.
- 2.6** This non-smoking policy applies to college facilities used by off-campus groups as well as college groups.

3. DISTRIBUTION

The terms of this policy will be posted on the Lamar State College – Port Arthur web page. The policy is available to all current employees and 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 Lamar State College - Port Arthur Catalog.

POLICY: ACQUIRED IMMUNE DEFICIENCY SYNDROME
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.15
REVISED: MARCH 15, 2002

Acquired Immune Deficiency syndrome (AIDS) is a fatal disease which has become a nationwide public health problem.

Lamar State College - Port Arthur acknowledges the seriousness of this problem. In health related matters such as this, the college follows the guidelines of recognized authorities including the National Center for Disease Control, the United States Public Health Service, the Texas Department of Health, and American College Health association. Further, the College will conform its actions to the Texas Communicable Disease Prevention and Control Act and other law.

There is no current evidence that individuals infected with Human Immunodeficiency Virus (HIV), the "AIDS Virus," can infect other individuals by casual contact. Accordingly, there is no reason to exclude individuals with the Acquired Immunodeficiency Syndrome (AIDS), AIDS-social, or cultural activities. Therefore, on the basis of current knowledge of the disease, individuals sharing common living space, work or study areas, libraries, classrooms, recreational facilities, and theaters do not represent a problem or public threat to the campus community.

Students and employees of the College who may become infected with the AIDS virus will not be excluded from enrollment or employment, or restricted in their access to College services or facilities, unless medically-based judgments in individual cases establish that exclusion or restriction is necessary to the welfare of the individual or of other members of the College community.

When circumstances arise that require review, the President will seek the advice of the attending physician, knowledgeable medical personnel, and other relevant parties. An opportunity will be provided for any person involved to discuss his or her circumstances. A College Health Committee will be appointed to review the issues and provide recommendations to the President for resolution.

In the event of public inquiry concerning College policy, programs, problems, or statistics related to AIDS on campus, the President will serve as the official spokes person for the College and will enlist the cooperation of the Coordinator of Public Information as necessary to prepare an appropriate response. All inquiries from the press, elected public officials, or the public in general will be referred to the spokesperson. The medical records of individuals shall remain confidential, but public information shall be disclosed upon request in accordance with the Texas Open Records Act, the Family Education Rights and Privacy Act, and the Texas Communicable Disease Prevention and Control Act. General information and national statistics considered public knowledge are not subject to restriction.

In the event an individual is identified with AIDS, ARC, or a positive test for HIV antibody, appropriate existing College resources for emotional, educational, social, and medical support will be made available to all concerned individuals.

Persons who know, or have reasonable basis for believing, that they are infected with the AIDS virus are expected to seek expert advice about their health circumstances and are obligated, ethically, legally, to conduct themselves responsibly in accordance with knowledge for the protection of other members of the College community.

The College shall carefully observe the safety guidelines established by the U.S. Public Health Services for the handling of blood and other body fluids and secretions, both in all health care facilities maintained on the campus and in other institutional contexts in which such fluids or secretions may be encountered (e.g. teaching and experimental laboratories).

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

I. Overview

A. Introduction

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

B. Purpose and Scope

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

C. References

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

II. Roles and Responsibilities

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

A. Generic Roles

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

1. Owner

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

2. Custodian

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

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

3. Agent

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

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

4. User

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

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

B. Specific Responsibilities

1. College President

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

2. Information Resources Manager (IRM)

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

3. Information Technology Personnel

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

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

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

directed to the Registrar's Office (the designated custodian of official transcript information).

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

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

4. Other College Personnel

a. Managers

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

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

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

b. Security Administrator

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

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

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

c. Other Personnel

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

5. Internal Audit Personnel

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

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

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

III. Security Violations and Sanctions

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

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

A. Detecting and Reporting

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

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

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

B. Sanctions

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

C. Disciplinary Actions

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

IV. Disaster Recovery/Business Continuity Plan

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

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

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

V. Information Resources Policies

A. Information Resources Security Policies

5.16.1 Physical Security Policy

5.16.1.1 Introduction

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

5.16.1.2 Purpose

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

5.16.1.3 Audience

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

5.16.1.4 Policy

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

access with a sign in/out log.

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

5.16.1.5 Supporting Information

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

5.16.2 Change Management Policy

5.16.2.1 Introduction

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

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

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

5.16.2.2 Purpose

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

5.16.2.3 Audience

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

5.16.2.4 Policy

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

during special events.

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

5.16.2.5 Supporting Information

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

5.16.3 Information Systems Privacy Policy

5.16.3.1 Introduction

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

5.16.3.2 Purpose

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

5.16.3.3 Audience

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

5.16.3.4 Ownership

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

5.16.3.5 Policy

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

5.16.3.6 Public Access Privacy Policy

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

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

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

I. Cookies

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

Any information that Lamar State College - Port Arthur web servers may store in cookies is used for internal purposes only. Cookie data is not used in any way that would disclose personally identifiable information to outside parties unless Lamar State College - Port Arthur is legally required to do so in connection with law enforcement investigations or other legal proceedings.

II. Logs and Network Monitoring

Lamar State College - Port Arthur maintains log files of all access to its site and also monitors network traffic for the purposes of site management. This information is used to help diagnose problems with the server and to carry out other administrative tasks. Log analysis tools are also used to create summary statistics to determine which information is of most interest to users, to identify system problem areas, or to help determine technical requirements.

Information such as the following is collected in these files:

Hostname: the hostname and/or IP address of the computer requesting access to the site

User-Agent: the type of browser, its version, and the operating system of the computer requesting access (e.g., Netscape 4 for Windows, IE 4 for Macintosh, etc.)

Referrer: the web page the user came from

System date: the date and time on the server at the time of access

Full request: the exact request the user made

Status: the status code the server returned, e.g., fulfilled request, file not found

Content length: the size, in bytes, of the file sent to the user

Method: the request method used by the browser (e.g., post, get)

Universal Resource Identifier (URI): the location of the particular resource requested and commonly known as a URL.

Query string of the URI: anything after a question mark in a URI. For example, if a keyword search has been requested, the search word will appear in the query string.

Protocol: the technical protocol and version used, i.e., http 1.0, ftp, etc.

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

III. Email and Form Information

If a member of the general public sends Lamar State College - Port Arthur an e-mail message or fills out a web-based form with a question or comment that contains personally identifying information, that information will only be used to respond to the request and analyze trends. The message may be redirected to another government agency or person who is better able to answer your question. Such information is not used in any way that would reveal personally identifying information to outside parties unless System Administration is legally required to do so in connection with law enforcement investigations or other legal proceedings.

IV. Links

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

V. Security

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

Contacting Lamar State College - Port Arthur

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

Samir.Ghorayeb@lamarpa.edu

5.16.3.7 Supporting Information

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

5.16.4 Security Training Policy

5.16.4.1 Introduction

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

5.16.4.2 Purpose

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

5.16.4.3 Audience

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

5.16.4.4 Policy

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

5.16.4.5 Supporting Information

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

5.16.5 Security Monitoring Policy

5.16.5.1 Introduction

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

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

5.16.5.2 Purpose

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

5.16.5.3 Audience

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

5.16.5.4 Policy

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

- The following checks will be performed at least annually by assigned individuals:
 - ❖ Password strength
 - ❖ Unauthorized network devices
 - ❖ Unauthorized personal web servers
 - ❖ Unsecured sharing of devices
 - ❖ Unauthorized modem use
 - ❖ Operating System and Software Licenses

- Any security issues discovered will be reported to the ISO for follow-up investigation.

5.16.5.5 Supporting Information

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

5.16.6 Intrusion Detection Policy

5.15.6.1 Introduction

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

5.16.6.2 Purpose

Intrusion detection provides two important functions in protecting information resources:

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

5.16.6.3 Audience

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

5.16.6.4 Intrusion Detection Policy

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

5.15.6.5 Supporting Information

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

5.16.7 Incident Management Policy

5.16.7.1 Introduction

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

5.16.7.2 Purpose

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

5.16.7.3 Audience

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

5.16.7.4 Incident Management Practice Standard

- Lamar State College - Port Arthur CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The ISO, working with the IRM, will determine if a widespread Lamar State College - Port Arthur communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
- The Lamar State College - Port Arthur ISO is responsible for reporting the incident to the:
 - ❖ IRM
 - ❖ Department of Information Resources as outlined in TAC 202
 - ❖ Local, state or federal law officials as required by applicable statutes and/or regulations

- The ISO is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.
- In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and Lamar State College - Port Arthur.

5.16.7.5 Supporting Information

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

5.16.8 Network Access Policy

5.16.8.1 Introduction

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

5.16.8.2 Purpose

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

5.16.8.3 Audience

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

5.16.8.4 Policy

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

5.16.8.5 Supporting Information

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

5.16.9 Network Configuration Policy

5.16.9.1 Introduction

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

5.16.9.2 Purpose

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

5.16.9.3 Audience

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

5.16.9.4 Policy

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

from Lamar State College - Port Arthur Information Technology.

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

5.16.9.5 Supporting Information

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

5.16.10 Server Hardening Policy

5.16.10.1 Introduction

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

5.16.10.2 Purpose

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

5.16.10.3 Audience

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

5.16.10.4 Policy

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

5.16.10.5 Supporting Information

This Policy is supported by the following Security Policy Standards references 8, 11, 16, and 17 in appendix D.

5.16.11 Account Management Policy

5.16.11.1 Introduction

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

5.16.11.2 Purpose

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

5.16.11.3 Audience

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

5.16.11.4 Policy

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

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

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

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

5.16.11.5 Supporting Information

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

5.16.12 Administrator/Special Access Policy

5.16.12.1 Introduction

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

5.16.12.2 Purpose

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

5.16.12.3 Audience

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

5.16.12.4 Policy

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

5.16.12.5 Supporting Information

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

5.16.13 Password Policy

5.16.13.1 Introduction

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

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

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

5.16.13.2 Purpose

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

5.16.13.3 Audience

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

5.16.13.4 Policy

- All passwords, including initial passwords, must be constructed and implemented according to the following Lamar State College - Port Arthur IR rules:
 - ❖ it must be routinely changed
 - ❖ it must adhere to a minimum length as established by Lamar State College - Port Arthur Information Technology
 - ❖ it must be a combination of alpha and numeric characters
 - ❖ it must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
 - ❖ it must not be dictionary words or acronyms
 - ❖ password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. Lamar State College - Port Arthur Information Technology personnel and Information Technology contractors will not ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Lamar State College - Port Arthur.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Lamar State College - Port Arthur ISO. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.

- Information Technology Helpdesk password change procedures must include the following:
 - ❖ authenticate the user to the helpdesk before changing password
 - ❖ change to a strong password
 - ❖ the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
 - ❖ Take control of the passwords and protect them
 - ❖ Report the discovery to the Lamar State College - Port Arthur Help Desk
 - ❖ Transfer the passwords to an authorized person as directed by the Lamar State College - Port Arthur ISO

Password Guidelines

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

Creating a strong password

- Combine short, unrelated words with numbers or special characters. For example: eAt42peN
- Make the password difficult to guess but easy to remember

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

5.16.13.5 Supporting Information

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

5.16.14 Portable Computing Policy

5.16.14.1 Introduction

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

5.16.14.2 Purpose

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

5.16.14.3 Audience

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

5.16.14.4 Policy

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

5.16.14.5 Supporting Information

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

5.16.15 Vendor Access Policy

5.16.15.1 Introduction

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

5.16.15.2 Purpose

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

5.16.15.3 Audience

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

5.16.15.4 Policy

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

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

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

5.16.15.5 Supporting Information

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

5.16.16 Backup Policy

5.16.16.1 Introduction

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

5.16.16.2 Purpose

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

5.16.16.3 Audience

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

5.16.16.4 Services

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

5.16.16.5 Policy

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

5.16.16.6 Supporting Information

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

5.16.17 Virus Protection Policy

5.16.17.1 Introduction

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

5.16.17.2 Purpose

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

5.16.17.3 Audience

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

5.16.17.4 Policy

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

5.16.17.5 Supporting Information

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

5.16.18 System Development Policy

5.16.18.1 Introduction

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

5.16.18.2 Purpose

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

5.16.18.3 Audience

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

5.16.18.4 Policy

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

5.16.18.5 Supporting Information

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

B. Information Resources Use Policies

5.16.19 Acceptable Use Policy

5.16.19.1 Introduction

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

5.16.19.2 Purpose

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

5.16.19.3 Audience

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

5.16.19.4 Ownership of Electronic Files

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

5.16.19.5 Privacy

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

5.16.19.6 Policy

- Users must report any weaknesses in Lamar State College - Port Arthur computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on Lamar State College - Port Arthur systems for which they do not have authorization or explicit consent.
- Users must not divulge dialup or dial back modem phone numbers to anyone.
- Users must not share their Lamar State College - Port Arthur account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. Users must not make unauthorized copies of copyrighted software.
- Users must not use non-standard shareware or freeware software without Lamar State College - Port Arthur Information Resources management approval unless it is on the Lamar State College - Port Arthur standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized

Lamar State College - Port Arthur user access to a Lamar State College - Port Arthur resource; obtain extra resources beyond those allocated; circumvent Lamar State College - Port Arthur computer security measures.

- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Lamar State College - Port Arthur users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Lamar State College - Port Arthur Information Resources.
- Lamar State College - Port Arthur Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which Lamar State College - Port Arthur may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the Lamar State College - Port Arthur official processes for dealing with academic ethical issues).
- Access to the Internet from a Lamar State College - Port Arthur owned, home based, computer must adhere to all the same policies that apply to use from within Lamar State College - Port Arthur facilities. Employees must not allow family members or other non-employees to access Lamar State College - Port Arthur computer systems.
- Users must not otherwise engage in acts against the aims and purposes of Lamar State College - Port Arthur as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use

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

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

5.16.19.7 Supporting Information

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

5.16.20 Internet Policy

5.16.20.1 Introduction

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

5.16.20.2 Purpose

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

5.16.20.3 Audience

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

5.16.20.4 Ownership

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

5.16.20.5 Privacy

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

5.16.20.6 Policy

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

Lamar State College - Port Arthur Acceptable Use Policies.

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

Incidental Use

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

5.16.20.7 Supporting Information

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

5.16.21 E-Mail Policy

5.16.21.1 Introduction

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

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

5.16.21.2 Purpose

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

5.16.21.3 Audience

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

5.16.21.4 Policy

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

College - Port Arthur information through non-Lamar State College - Port Arthur E-Mail accounts. Examples of non-Lamar State College - Port Arthur E-Mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and E-Mail provided by other Internet Service Providers (ISP).

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

5.16.21.5 Supporting Information

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

5.16.22 Instant Messaging Policy

5.16.22.1 Introduction

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

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

5.16.22.2 Purpose

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

5.16.22.3 Audience

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

5.16.22.4 Policy

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

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

5.16.22.5 Supporting Information

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

5.16.23 Peer-to-Peer (P2P) Policy

5.16.23.1 Introduction

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

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

5.16.23.2 Purpose

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

5.16.23.3 Audience

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

5.16.23.4 Policy

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

specifically authorized in writing by the Director of Information Technology Services.

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

5.16.23.5 Supporting Information

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

5.16.24 Software Licensing Policy

5.16.24.1 Introduction

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

5.16.24.2 Purpose

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

5.16.24.3 Audience

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

5.16.24.4 Policy

- Lamar State College - Port Arthur provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information or software, that Lamar State College - Port Arthur does not have specific approval to store and/or use, must not be stored on Lamar State College - Port Arthur systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).
- Third party software in the possession of Lamar State College - Port Arthur must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes. Manuals, and other copyrighted materials, shall not be copied without specific, written permission of the publisher.
- Permission is granted to users for the use of licensed software according to the regulations set forth herein by Lamar State College - Port Arthur for the use of such software. The use of such software is governed by the terms of licensing agreements between the College and the software licensors, and the user must read and abide by the terms of those agreements.
- Computer software shall be used in strict accordance to its licensing agreement. By way of example only, such agreements may prohibit the copying of software from one computer to another or the making of unauthorized copies to install on computers not owned or controlled by the College.
- Most software is proprietary and may therefore be subject to copyright or patent restrictions as defined in the license agreements.
- Users may make only one backup copy of the software for archival purposes. If the underlying license is discontinued, this copy must be destroyed. Otherwise, users must not copy, disclose, transfer, or remove any proprietary programs from the media on which the software resides.
- Users must not use Lamar State College - Port Arthur equipment or software to violate the terms of any software license agreement. Information on specific software licenses on all public computer systems can be obtained from the Information Technology Department.
- Software for which the College holds the license may not be copied or removed from a College-owned computer and placed on another College-owned computer or any computer owned by any other person or entity.
- Ordinarily, the College must own or hold the license for any software loaded onto a College-owned computer.
- An individual user may request that the Information Technology Department install software that, while not purchased or licensed by the College, the user can utilize for business or instructional purposes. In this case the user must demonstrate or certify the purchase or license of the software. The decision to load software that is not owned by the College rests with the Director of Information Technology Services.
- The Information Technology Department reserves the right to audit any personal computer on College property-regardless of whether or not the equipment is owned, operated, or controlled by the College-at any time for unauthorized software.
- These rules also govern shareware and freeware programs that can be obtained from Internet access. All programs coming from Internet sources must be approved for use and be installed by the Information Technology Department.

- All software should be scanned for viruses before use.
- Standardized Internet access software such as browsers, graphics converters, etc. shall be provided by the Information Technology Department. These programs will have been tested and found to be virus free.
- Software loaded on College-owned computers must support the mission of the College and should have the primary purpose of assisting the user to perform legitimate job functions.
- The Information Technology Department shall load all software on all equipment for which it has direct responsibility. The Information Technology Department shall not support any software that it did not install and shall not install software that it feels it cannot adequately support.
- Lamar State College - Port Arthur software applications shall not be used to create, modify, access, view, display, or activate files, information, or materials that are offensive, indecent, or illegal.
- Each manufacturer includes a license agreement package with its software that details any restrictions on its use. Users must comply with the vendor's license provisions regarding the use of the software, even though the individual user has not personally signed the license agreement. License agreements differ among the various software vendors and some may grant additional rights, such as allowing use on a portable or home computer. The College shall hold each user responsible for reading, understanding, and complying with provisions of the license agreement for each software package.

5.16.24.5 Supporting Information

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

5.16.25 Computing Facilities Use Policy

5.16.25.1 Introduction

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

5.16.25.2 Purpose

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

5.16.25.3 Audience

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

5.16.25.4 Policy

- Users shall be accountable for using computing facilities in an effective, ethical and lawful manner.
- Users must not use Lamar State College - Port Arthur's computer systems, including any of its communications facilities and services, in any way which deliberately diminishes or interferes with the reasonable and confidential use of those systems for College business by others, or which is intended to do the same. Lamar State College - Port Arthur retains the right to access and remove immediately any data or files evidencing any such misuse.
- The Information Technology Department must approve all access to the College's central computer systems. Department heads must approve all access to computer systems under their direct control.
- Account access information assigned to an individual for use of the central computers or departmental systems is not to be given to another individual. The individual assigned an account is responsible for all activity for which that account is used. Use of another person's account is not only a violation of College policy; it is a violation of state law.
- Computing facilities and accounts are owned by the College and are to be used for College-related activities only.
- Users are expected to abide by the security restrictions on all systems and information to which they have access.
- Programs and files are confidential, and may only be accessed by those persons authorized to do so.
- Please be sensitive to the inherent limitations of shared network resources. No computer security system can prevent a determined person from gaining unauthorized access to stored information. Good judgment dictates the creation of electronic documents that, should they become available to the public, will not bring embarrassment or liability to the College or its constituencies.
- Use of College computing facilities to create, display, modify, or transmit files that are abusive, harassing, threatening, indecent, or illegal is expressly prohibited.
- Material that might be considered indecent, abusive, harassing, or threatening may be accessed, activated, and viewed only insofar as those materials and resources are required to perform legitimate job functions. However, caution must be exercised to avoid displaying the material in any way that might interfere with the performance of

other employees or that creates an intimidating, hostile, or offensive workplace or academic environment.

- Illegal material may not be used to perform any legitimate job function and therefore may not be accessed, viewed, or stored on College computing facilities.
- Users are expected to promote efficient use of network resources consistent with the instructional, research, public service and administrative goals of the College. Users must display consideration for others and refrain from engaging in any use that would interfere with their work or disrupt the intended use of network resources. Wasteful and disruptive practices such as sending chain letters, broadcast messages or unwanted material are specifically prohibited.
- Conduct that involves the use of computing or communications resources to violate a College policy or regulation, or to violate another's rights, is a serious abuse and can result in limitation of privileges and lead to appropriate disciplinary action.

5.16.25.5 Supporting Information

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

5.16.26 Telephone Systems Policy

5.16.26.1 Introduction

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

5.16.26.2 Purpose

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

5.16.26.3 Audience

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

5.16.26.4 Policy

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

5.16.26.5 Supporting Information

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

VI. Appendices

Appendix A: Administrative Systems Assets/Custodians

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

Asset Name/Application	Asset Description	Asset Custodian
SunGard H.E. PLUS FRS	Financial Records System, Purchasing, Accounts Payable, BDS (budget) and Interfaces Systems	<ul style="list-style-type: none"> • VP for Finance
SunGard H.E. PLUS HRS	Human Resources System, Personnel, Payroll, Position Control/Budget Systems	<ul style="list-style-type: none"> • Human Resources Director • Payroll Director • Associate VP for Finance
SunGard H.E. PLUS SIS	Student Information Systems - Student Records, Admission, Financial Aid Systems	<ul style="list-style-type: none"> • VP for Student Services
SunGard H.E. PLUS SIS	Student Information System Billing and Receivables System	<ul style="list-style-type: none"> • VP for Finance

Appendix B: Information Resources Policies Maintenance

The maintenance of this Manual will be the responsibility of the Director of Information Technology Services. Changes will be made to the Manual as necessitated by federal and state laws as well as changes in the College policies.

Notices of any changes to the Manual will be disseminated campus-wide.

Appendix C: Definitions

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

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

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

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

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

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

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

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

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

Change can consist of any or all of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vendor: someone who exchanges goods or services for money.

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

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

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

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

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

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A

worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Appendix D: Standard Policy Statements

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

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

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

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

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

POLICY: WHISTLE BLOWER
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.17
REVISED: MARCH 15, 2002; DECEMBER 22, 2005

A state agency or institution may not take action against an employee who, in good faith, reports a violation of the law to law enforcement. (Texas Government Code, Section 554.002) An employee who alleges a violation of this provision may file suit against the State, but such action must be taken no later than 90 days after the violation occurred or was discovered. The employee also must exhaust the appeals process during this 90-day period. (Texas Government Code, Section 554.003, Section 554.004, and Section 554.006)

POLICY: OPEN RECORDS ACT
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.18
REVISED: MARCH 15, 2002

The Texas Open Records Act became effective June 14, 1973. Its purpose is stated in section 552.001 of the Act:

. . . each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees.

Section 552.024 of the Act requires each employee or official of a governmental body and each former employee or official of a governmental body to choose whether to allow public access to information in the custody of the governmental body, such as: (1) home address, (2) home telephone number, (3) social security number, or (4) information that reveals whether a person has family members. If an employee fails to declare this information as confidential in compliance with this section, the information will be subject to public access.

Lamar State College - Port Arthur employees make the election whether or not to have this information remain confidential when he or she completes the Personnel Event Form at the inception of employment. Should the employee wish to change his/her election subsequently, a new Personnel Event Form must be completed.

(Texas Gov't Code Ann., Section 552.001)

POLICY: SEXUAL HARASSMENT
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.19
REVISED: DECEMBER 10, 2003

1. POLICY

It is the policy of Lamar State College - Port Arthur that no employee, student, or contractor of the College may sexually harass another person. Any employee, student, or contractor will be subject to disciplinary action up to and including dismissal for a violation of this policy. Rules and Regulations, the Texas State University System, VII.8.0

Lamar State College - Port Arthur strives to provide an educational and working environment for its students, faculty, and staff free of intimidation and harassment. Sexual harassment is sex discrimination and is, therefore, a violation of the 1964 Civil Rights Act.

2. DISTRIBUTION OF POLICY

This policy is available on The Human Resources web page.

3. TRAINING

Lamar State College - Port Arthur is mandated to provide Sexual Harassment training to each new employee on policies regarding harassment no later than 30 days after the date of hire. Each new employee is provided training during new employee orientation. Through brochures, training, and other appropriate means, the Human Resources Office will provide information to employees concerning the following: (1) definitions of sexual harassment; (2) examples of incidents of sexual harassment; (3) descriptions of how and when to report sexual harassment; (4) descriptions of available informal and formal resolution mechanisms; (5) sources of support and information for victims and respondents. In addition, supplemental training is held every two years. A signed statement verifying attendance is required to be maintained in the employee=s personnel file.

4. DEFINITION

Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when:

1. Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment or academic career.
2. Submission to or rejection of such conduct by an individual is used as the basis for employment or academic decisions affecting the individual.
3. Such conduct has the purpose or effect of unreasonably interfering with an individual's performance or creating an intimidating, hostile, or offensive employment or academic environment.
4. Submission to or rejection of such conduct by a student is used as a basis for evaluating such student's academic performance.
5. Such conduct has the purpose of unreasonably interfering with a student's academic or extracurricular activity or creating an intimidating, hostile, or offensive environment.

5. COMPLAINTS

In determining whether alleged conduct constitutes sexual harassment, Lamar State College - Port Arthur shall construe any act or omission within the totality of circumstance, such as the nature of the conduct and the context in which the alleged incidents occurred.

Lamar State College - Port Arthur may not dismiss a complaint once registered with the appropriate authority until the case has been resolved. **The Director of Human Resources and the appropriate Vice President or Dean will continue to monitor the circumstances surrounding the complaint to ensure the situation has been remedied. The College may take immediate and appropriate disciplinary action for any sexual harassment occurring in the employment or academic environment even in the absence of an individual complaint.** Disciplinary action may consist of action up to and including termination of employment or, in the case of a student, dismissal from the College. If disciplinary action is imposed for engaging in sexual harassment, the individual may invoke the applicable due process procedures.

To the fullest extent practicable, Lamar State College - Port Arthur shall keep complaints of sexual harassment and the terms of their resolution confidential.

5.1 INFORMAL COMPLAINTS: All complaints are considered informal until they are filed in writing. The steps for seeking an informal resolution are as follows:

- 5.1.1** The offended individual should report the incident(s) to the Vice President for Academic Affairs if the complaint is against a faculty member, the Vice President of Student Services if the complaint is against a student or the appropriate Department head if the complaint is against a staff member. Complaints against the employee=s direct supervisor may be filed with any other of the above officials. Any employee contacted about an alleged sexual harassment incident is required to then notify the Director of Human Resources.
- 5.1.2** The college official will work with the complainant to determine the extent of the alleged sexual harassment.
- 5.1.3** The evidence presented will be reviewed to determine if there is cause to believe that a sexual harassment violation occurred.
- 5.1.4** If in the judgment of the college official a violation did not occur, the complainant will be so advised and given a verbal explanation of why the incident(s) described does not constitute sexual harassment.
- 5.1.5** If the complainant does not agree with this decision, the complainant will be given the opportunity to file a formal written complaint.
- 5.1.6** If the college official has cause to believe sexual harassment did occur, the complainant will be given the option of filing a formal complaint or pursuing an informal resolution.
- 5.1.7** If the complainant chooses to pursue the informal resolution, the resource person will notify the person being charged that an informal complaint has been filed against him/her and the complainant wishes to seek an informal resolution to the problem. The charged party will be given an opportunity to confirm or rebut the charge. The resource person will then meet with both parties together or independently and try to reach a mutually agreeable resolution.
- 5.1.8** If a resolution is not achieved, the charging party will be given the opportunity to file a written formal complaint.
- 5.1.9** The College may elect to pursue the charge even if the complainant does not elect to proceed.

5.2 FORMAL COMPLAINT

To be considered a formal complaint; the complaint must be submitted to the appropriate person in writing within ninety (90) days of the most recent incident and must include the resolution being sought. Complaints

filed against a faculty member should be directed to the Vice President for Academic Affairs, complaints against a staff member should be directed to the appropriate Division head; and complaints against a student should be directed to the Vice President of Student Services. **Complaints may be filed with any College official.** Any employee contacted about a complaint of sexual harassment should immediately contact the Director of Human Resources. Appeals must be filed within five (5) working days of receiving an answer and each step should be completed within ten (10) working days.

5.2.1 Step One

- a. The college official will review the written complaint with the charging party.
- b. If the college official person does not feel there is cause to believe that sexual harassment occurred, he/she will so advise the complainant in writing stating the reason(s) for the decision.
- c. If the college official thinks there is cause to believe that sexual harassment did occur, he will notify the charged party that he/she has been formally charged with sexual harassment and give him/her a copy of the written charge. The accused party will be given the opportunity to confirm or rebut the charge in writing.
- d. The college official will then meet with both parties either together or separately and try to reach a mutually agreeable resolution.

5.2.2 Step Two

- a. If a solution is not reached in Step One, the college official and the Director of Human Resources will meet with both parties, either together or separately, to review both sides of the issue.
- b. The college official person and the Director of Human Resources will then mutually agree on a resolution which will be communicated in writing to both parties.
- c. Both parties will be instructed by the Director of Human Resources to comply with the terms of the resolution.

5.2.3 Step Three

- a. The decision may be appealed by either party to the President by submitting a written statement to the Director of Human Resources. The appeal must include the basis for the appeal and the remedy sought.
- b. The President will take whatever action he feels appropriate to resolve the complaint. The President's decision is final and binding.
- c. If a complaint, whether informal or formal, is filed against a college official or the Director of Human Resources, the functions assigned to the person by these procedures will transfer to the President or his designee.
- d. The complainant and the respondent both have the right to bring an advisor to the meeting. The advisor may not act as a participant, but may render consultation to the advisee. If either party chooses to exercise this option, he/she shall submit the name of the advisor in writing to the Director of Human Resources at least forty-eight (48) hours prior to the meeting.

6. RETALIATION

Retaliation or reprisal by the College or by any member of the College community against anyone who in good faith has articulated a concern about harassment, resisted harassment, participated or cooperated in a complaint investigation or hearing or filed a complaint alleging harassment is illegal. Such retaliation is also prohibited by this policy. Prohibited retaliatory conduct includes, but is not limited to changing work or class assignments, or otherwise interfering with work or school performance. Retaliatory conduct is grounds for appropriate disciplinary action, up to and including discharge or expulsion.

POLICY: RACIAL HARASSMENT
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.20
REVISED: MARCH 15, 2002

1. POLICY

Lamar State College - Port Arthur shall provide equal educational opportunities for all students and equal employment opportunities for all applicants and employees and otherwise foster and environment free of racial intimidation, humiliation, and harassment. Racial harassment, as defined herein, is expressly prohibited. Rules and Regulations, the Texas State University System, Section VII-7.0

"Racial Harassment" is defined as extreme or outrageous acts or communications that are intended to harass, intimidate, or humiliate students, faculty, staff or visitors on account of race, color, or national origin and that reasonably cause them to suffer severe emotional distress. It is a violation of this policy for any student, faculty, or staff member to engage in racial harassment of any person on campus or in connection with a college sponsored activity.

It is a violation for any student, faculty or staff member to use authority granted by state law, by system rule, or by college policy to deprive any person of his or her civil rights on campus or in connection with a college sponsored activity.

If a violation of this policy is committed on campus or in connection with a college sponsored activity because of the race, color or national origin of any person harmed by such violation, the violator's discriminatory purpose shall be treated as an aggravating factor for the purpose of determining the appropriate penalty.

Student, faculty and staff member offenders are subject to disciplinary action as appropriate under the circumstances up to and including dismissal for violation of this policy.

2. COMPLAINT

Any employee, student or visitor who thinks he/she is the victim of racial harassment should lodge a complaint against the offender. A complaint should be filed with the appropriate College official 1) the Vice President for Academic Affairs if it is against a faculty member 2) the appropriate Division head if it is against a staff member or 3) the Vice President of Student Services if it is against a student. **Complaints may be filed with any College official.** Any employee contacted about a complaint of racial harassment should immediately contact the Director of Human Resources.

2.1 INFORMAL COMPLAINT

All complaints are considered informal until they are filed in writing. The steps for seeking an informal resolution are as follows:

- 2.1.1** The offended individual should report the incident(s) to the appropriate College official or the Director of Human Resources.
- 2.1.2** The college official will work with the complainant to determine what evidence exists for the charge of racial harassment.
- 2.1.3** The evidence presented will be reviewed to determine if there is cause to believe a violation of racial harassment occurred.
- 2.1.4** If in the judgment of the college official a violation did not occur, the complainant will be so advised and given a verbal explanation of why the incident(s) described does not constitute racial harassment.

- 2.1.5 If the complainant does not agree with this decision, the complainant will be given the opportunity to file a formal written complaint.

2.2 FORMAL COMPLAINT

If the college official has cause to believe racial harassment did occur, the complainant will be given the opportunity to file a formal complaint or pursue an informal resolution.

- 2.2.1 If the complainant chooses to pursue the informal resolution, the resource person will notify the person charged that an informal complaint has been filed against him/her and the complainant wishes to seek an informal resolution to the problem. The charged party will be given an opportunity to confirm or rebut the charge. The resource person will then meet with both parties together or independently and try to reach a mutually agreeable resolution.

- 2.2.2 If a resolution is not achieved, the charging party will be given the opportunity to file a written formal complaint.

- 2.2.3 The College may elect to pursue the charge even if the complainant does not elect to proceed.

- 2.2.4 To be considered a formal complaint; the complaint must be submitted to the appropriate college official in writing within ninety (90) days of the most recent incident and must include the resolution being sought. A complaint should be filed with 1) the Vice President for Academic Affairs if it is against a faculty member 2) the appropriate Division head if it is against a staff member or 3) the Vice President of Student Services if it is against a student. Complaints may be filed with any College official. Any employee contacted about a complaint of racial harassment should immediately contact the Director of Human Resources. Appeals must be filed within five (5) working days of receiving an answer and each step should be completed within ten (10) working days.

2.2.5 Step One

- a. The college official will review the written complaint with the charging party.
- b. If the college official does not feel there is cause to believe that racial harassment occurred, he/she will so advise the complainant in writing stating the reason(s) for the decision.
- c. If the college official thinks there is cause to believe that racial harassment did occur, he/she will notify the charged party that he/she has been formally charged with racial harassment and give him/her a copy of the written charge. The accused party will be given the opportunity to confirm or rebut the charge in writing.
- d. The college official will then meet with both parties either together or separately and try to reach a mutually agreeable resolution.

2.2.6 Step Two

- a. If a solution is not reached in Step One, the college official and the Director of Human Resources will meet with both parties, either together or separately, to review both sides of the issue.
- b. The college official and the Director of Human Resources will then mutually agree on a resolution which will be communicated in writing to both parties.

- c. Both parties will be instructed by the Human Resources to comply with the terms of the resolution.

2.2.7 Step Three

- a. The decision may be appealed by either party to the President by submitting a written statement to the Director of Human Resources. The appeal must include the basis for the appeal and the remedy sought.
- b. The President will take whatever action he feels appropriate to resolve the complaint. The President's decision is final and binding.
- c. Lamar State College - Port Arthur may take appropriate disciplinary action for any racial harassment occurring in the employment or academic environment even in the absence of an individual complaint. Disciplinary action may consist of action up to and including termination of employment or, in the case of a student, dismissal from the College. If disciplinary action is imposed, the accused shall have his/her full right to invoke applicable due process procedures.
- d. If a complaint, whether informal or formal, is filed against a college official or the Director of Human Resources, the functions assigned to the person by these procedures will transfer to the President or his designee.
- e. The complainant and the respondent both have the right to bring an advisor to the meeting. The advisor may not act as a participant, but may render consultation to the advisee. If either party chooses to exercise this option, he/she shall submit the name of the advisor in writing to the Director of Human Resources at least forty eight (48) hours prior to the meeting.

3. RETALIATION

Under no circumstances will Lamar State College - Port Arthur permit retaliation against an individual in any way as result of seeking relief under this policy.

POLICY: PROHIBITION OF WEAPONS
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.21
REVISED: DECEMBER 22, 2005

1. POLICY

It is a violation of the Texas State University System Rules and Regulations to possess, carry or otherwise cause a firearm, handgun or other prohibited weapons as defined by the Texas Penal Code-licensed or otherwise to be brought on the premises of a System component.

APremises of a System component@ as used in this section means a structure and the land, including appurtenances, on which the structure is situated, over which this Board has ownership or control. Specifically, this includes, but is not limited to, System campuses, the System Administrative Office, leased facilities or other facilities when a System or campus function, event, or activity takes or is taking place. This prohibition shall not apply to academic programs or to college sponsored or approved events in which the college explicitly authorizes the use of handguns. Nor shall it be a violation of this rule to transport firearms and/or handguns for registration with and storage by the college public safety office.

POLICY: RECOGNITION OF SERVICE AND RETIREMENT
SCOPE: FACULTY AND STAFF
POLICY NUMBER: 5.22
APPROVED:
REVISED: JANUARY 4, 2006

1. POLICY

Lamar State College – Port Arthur offers recognition of service awards to employees who have completed career milestones of five or more years of service to the College and employees who retire under the provisions of the College’s Retirement Plan.

2. ELIGIBILITY

Regular full-time employees are eligible for employee recognition awards after completion of five year of College service and every five-year period thereafter.

1. Time spent on family medical leave will count toward service.
2. Employees not currently employed at the time of the awards ceremony are ineligible for an award.
3. Full time employees who retire under the provisions of the College’s Retirement Plan are eligible for a service award if the full required service time has been earned.
4. The awards program will recognize service to Lamar State College - Port Arthur in five (5) year increments; thus, awards shall be presented to employees with 5, 10, 15, 20, 25+ years of continuous service. The cost of each award shall not exceed that amount established by the State of Texas.
5. At the time of the award the employee must hold a full time or 100% FTE position.
6. Part-time Student Assistant, Student Work Study, hourly or part time employment will count toward Staff Awards service time.
7. Periods of leave (not including FML) will not be counted toward service time.