POLICY: **INFORMATION RESOURCES**
SCOPE: **FACULTY, STAFF, AND STUDENTS**
POLICY NUMBER: **5.16**
REVISED: **JANUARY 2013**

I. Overview

A. Purpose and Scope

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

B. Authority

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

II. Security Violations and Sanctions

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

A. Detecting and Reporting

Users of College information resources are expected to report any known or observed attempted security violation. Additionally, they must not conceal or help to conceal violations by any party. Any actual or suspected security violation should be reported immediately to the Director of Information Technology Services at 409-984-6484 or to the Assistant Director of Systems, Networking, and Telecom at 409-984-6141.

B. Disciplinary Actions

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

III. Information Resources Policies

5.16.1 Responsibilities
Authority – TAC 202.70; 202.71; 202.72; 202.75

1. The IRM shall produce annually for review and approval by the president of the college a document identifying college information resource ownership and associated responsibilities for all information resource assets. (TAC 202.71.a)
2. The IRM shall produce annually for review and approval by college information resource owners a document identifying information resource custodians and approved users. (TAC

202.71.c)

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

5.16.2 Data Classification and Risk Assessment

Authority-TAC 202.70; 202.71; 202.72; 202.74; 202.76

1. All data owners or designated custodians shall be responsible for classifying data processed by systems under their purview based on data sensitivity so that the appropriate security controls can be applied and the information resource can be appropriately managed. (TAC 202.71.c.1.I)
2. The Data Classification document produced annually by the ISO shall be used to identify data types and their need for confidentiality, integrity, and availability. (TAC 202.71.b, 202.76.a.3)
3. A data classification of Category-I shall be based on compliance with applicable federal or state law, a contract, or on the demonstrated need to: (TAC 202.71.b, 202.76.a.3)
   - Document the integrity of that digital data (that is, confirm that data was not altered intentionally or accidentally),
   - Restrict and document individuals with access to that digital data, and
   - Ensure appropriate backup and retention of that digital data.
4. Certain digital data not defined as Category-I digital data can be so classified if warranted by a department's demonstrated need. With suitable justification, the college may convert its classification of these digital data from Category-I digital data to a lesser classification upon request by the data owner, with IRM review and approval. (TAC 202.71.c.1.I, 202.72.c)
5. Under the guidance of the Information Security Officer, the college shall annually conduct and document an information security risk assessment. (TAC 202.72.a, 202.73.b, 202.74.a.2)
6. The confidentiality, integrity, and availability of information resources shall be managed and protected based on sensitivity and risk. (TAC 202.70.1)
7. The IRM produce and maintain a procedure manual consisting of IRM reviewed and approved procedures for the management and operation of information resource assets.

5.16.3 Physical and Environmental Security Policy

Authority-TAC 202.73; 202.75

1. All physical security and environmental control systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

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

5.16.4 Backup and Business Continuity
Authority-TAC 202.70; 202.74; 202.75

1. The IRM is responsible for developing and maintaining a Disaster Recovery Plan designed to address the operational restoration of the college's critical computer processing capability. The plan will integrate into and meet the objectives of the larger Business Continuity Plan for the college and be reviewed on the same schedule. (TAC 202.70.6, 202.74.a)
2. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner. (TAC 202.74.b)
3. The vendor(s) providing offsite backup storage, if any, for the college must be cleared to handle the highest level of information stored. (TAC 202.75.7.E)
4. Physical access controls implemented at offsite backup storage locations, if any, must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the college's highest sensitivity level of information stored. (TAC 202.75.7.E)
5. The backup and recovery process for each system must be documented and periodically

reviewed. (TAC 202.75.7.E)

6. A process must be implemented to verify the success of the college electronic information backup. (TAC 202.75.7.E)
7. Backups must be periodically tested to ensure that they are recoverable. (TAC 202.75.7.E)
8. Procedures between the college and the offsite backup storage vendor(s), if any, must be reviewed and approved periodically by the IRM. (TAC 202.75.7.E)

5.16.5 Portable Computing and Encryption
Authority-TAC 202.75

1. Only portable computing devices approved by the IRM may be used to access college information resources. (TAC 202.75.7.Q)
2. College owned portable computing devices must be password protected. (TAC 202.75.7.Q)
3. College data should not be stored on portable computing devices or portable storage devices/media. Specific, written permission shall be obtained from the data owner before a user may store Category-I college data on a portable computing or storage device/media. (TAC 202.75.7.Q)
4. Category-I/II college data shall not be copied to or stored on portable computing devices, portable storage device/media or non-college owned portable computing device in a non-encrypted state. (TAC 202.75.4, 202.75.7.H)
5. Category-I/II college data must not be transmitted on a public network or via wireless network unless approved encryption techniques and/or approved wireless transmission protocols are utilized. (TAC 202.75.4, 202.75.7.H, 202.75.7.Z.ii)
6. The ISO is responsible for determining the approved encryption methods for storing and transmitting college data. (TAC 202.75.4, 202.75.7.H, 202.75.7.Z.ii)
7. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or locked in a secure, out-of-sight area of a vehicle. (TAC 202.75.7.Q)

5.16.6 System Development and Auditing
Authority-TAC 202.71; 202.75; 216

1. The Information Technology Services Department is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for college system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; security implications; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical college information. (TAC 202.75.6.B, 202.75.7.D, 202.75.7.U, 202.75.7.W)
2. All production systems must have designated owners and custodians. The Director of Information Technology Services Department shall produce and maintain a Project Management Practices manual. The manual shall contain the methodology for managing information technology projects. The methodology shall include a definition of the varying classifications of projects, and the required components of the methodology for each project classification as required by the Department of Information Resources' Project Management Practices Rule §216. (TAC 202.71.c)
3. All production systems must have designated owners and custodians. (TAC 202.71.c)
4. All production systems must have an access control system suited to the classification of data stored on the system as determined by the risk analysis process. (TAC 202.75.3.C)
5. Where resources permit, there shall be a separation between the production, development, and test environments. All development and testing environments must utilize sanitized data or maintain the same security access as the production system. (TAC 202.75.6.A)

6. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production. (TAC 202.75.7.D)
7. Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of Category-I data. (TAC 202.75.5.A)
8. Appropriate audit trails shall be maintained to provide accountability for updates to Category-I data and related hardware and software, and for all changes to automated security or access rules. (TAC 202.75.5.B)
9. Based on the risk assessment completed by the ISO, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system. (TAC 202.75.5.C)
10. Where possible a logon banner/warning should be presented when a user logs on to a system. The ISO shall approve the content of the banner/warning. (TAC 202.75.9)

5.16.7 Acceptable Use
Authority – TAC 202.70; 202.75

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

where this aspect of the research has the explicit approval of the college's official processes for dealing with academic ethical issues). (TAC 202.75.7.L)

15. Illegal material may not be used to perform any legitimate job or academic function and therefore may not be created, accessed, stored, viewed, or transmitted on college information resources. (TAC 202.75.7.L)
16. A Lamar State College - Port Arthur owned, home based, computer must adhere to all the same policies that apply to use from within Lamar State College - Port Arthur facilities. Employees must not allow family members or other non-employees access to college computer systems. (TAC 202.75.7.A)
17. Users must not otherwise engage in acts against the aims and purposes of Lamar State College - Port Arthur as specified in its governing documents or in rules, regulations and procedures adopted from time to time. (TAC 202.75.7.A)
18. All user activity on college information resources assets is subject to logging, monitoring, and review. (TAC 202.75.7.A)
19. Privately owned information resources are subject to the Acceptable Use Policy when used or operated on campus. (TAC 202.75.7.A)
20. As a convenience to the Lamar State College - Port Arthur user community, some incidental use of information resources is permitted. The following restrictions apply: (TAC 202.75.7.A, 202.75.7.G, 202.75.7.L)
    a. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, telephones, and so on, is restricted to college approved users; it does not extend to family members or other acquaintances.
    b. Incidental use must not result in direct costs to the college.
    c. Incidental use must not interfere with the normal performance of an employee's work duties.
    d. No files or documents may be sent or received that may cause legal action against, or embarrassment to, the college.
    e. Storage of personal email messages, voice messages, files and documents within the college's information resources must be nominal.
    f. All messages, files and documents – including personal messages, files and documents – located on college information resources are owned by the college, may be subject to open records requests, and may be accessed in accordance with this policy.
    g. Non-business related purchases made over the internet are prohibited.

5.16.8 Account Management
Authority-TAC 202.71; 202.75; 202.77

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

202.75.7.X, 202.77.c)

5.16.9 Administrator/Special Access
Authority-TAC 202.75

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

5.16.10 Change Management Policy
Authority-TAC 202.70; 202.75

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

5.16.11 Incident Management
Authority-TAC 202.75; 202.76

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

5. The ISO is responsible for coordinating communications with outside organizations and law enforcement and act as the liaison between law enforcement and the college. (TAC 202.76.a, 202.76.c)
6. The ISO shall make monthly summary incident reports to the Department of Information Resources in the manner the department determines. (TAC 202.76.d)

5.16.12 Password Security Policy
Authority- TAC 202.75

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

5.16.13 Intrusion Detection
Authority-TAC 202.75

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

5.16.14 Network Access
Authority-TAC: 202.75; 202.77

1. Use of the college network constitutes acknowledgement of and agreement to abide by all policies set forth in the Acceptable Use Policy. (TAC 202.77.a, 202.77.b)

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

5.16.15 Network Management and Configuration
Authority- TAC 202.75

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

5.16.16 Information Resources Privacy Policy
Authority-TAC 202.75

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

authorities, allow institutional officials to fulfill their responsibilities when acting in their assigned capacity, and to perform audits. No notification is required to view this information; however, users with privileged access are expected to maintain the privacy of the individual. (TAC 202.75.7.R)

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

5.16.17 Security Monitoring
Authority-TAC 202.71; 202.75

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

5.16.18 Security Awareness and Training
Authority-TAC 202.75; 202.77

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

5.16.19 Server Management and Hardening
Authority-TAC 202.75

1. The IRM will create and maintain a server registration that will include the designated server owner and server administrator(s) and other information necessary to indicate the purpose and function of the server supports and is consistent with college initiatives.
2. A server owner shall be designated by the IRM for each server. The server owner shall be

responsible for establishing server usage policies, specifying server access controls (both physical and electronic), and assuring compliance with state and college server management standards. Data owners may be server owners.

3. A server administrator shall be designated by the server owner for each server. The server administrator shall be responsible for enforcing the owner's usage policies, implementing the owner-specified access controls, and configuring the server according to the required standards. Data custodians may be server administrators.
4. The IRM shall produce and maintain a server management guide that includes server management standards and best practices for college owned servers. All servers must be maintained to the standard set forth in the guide unless an exception has been made based on a documented risk management decision.
5. A server must not be connected to the college network until it is in an Information Technology Services Department accredited secure state and the network connection is approved by Information Technology Services Department. (TAC 202.75.7.U)
6. The degree of hardening for operating systems and applications shall be in accordance with the importance of the information on the system and the acceptable risk as determined by the data owner. (TAC 202.75.7.U)
7. Information Technology Services Department will monitor security issues, both internal to the college and externally, and will manage the release of security patches on behalf of the college. (TAC 202.75.7.U)
8. Information Technology Services Department may make hardware resources available for testing security patches in the case of special applications. (TAC 202.75.7.U)
9. Security patches must be implemented within the specified timeframe of notification from the Information Technology Services Department. (TAC 202.75.7.U)
10. Servers that pose an immediate threat to network operations, performance, or other network-connected devices must be disconnected or quarantined to minimize risk until the threat is removed.

5.16.20 Software Licensing
Authority-TAC 202.75

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

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

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

5.16.22 Vendor Access
Authority-TAC 202.75

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

5.16.23 Malicious Code
Authority-TAC 202.75

1. All workstations and servers, whether connected to the college network, or standalone, must use the Information Technology Services Department approved virus and malware protection software and configuration. (TAC 202.75.7.Y)
2. The virus and malware protection software must not be disabled or bypassed. (TAC 202.75.7.Y)
3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software. (TAC 202.75.7.Y)
4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates. (TAC 202.75.7.Y)
5. Any system identified as a security risk due to a lack of anti-malware software may be disconnected from the network, or the respective network account may be disabled, until adequate protection is in place. (TAC 202.75.7.Y)
6. Every virus that is not automatically cleaned or quarantined by the virus protection software must be reported to the Information Technology Services Department Help Desk. (TAC 202.75.7.Y)

5.16.24 Data Disposal and Destruction
Authority-TAC 202.78

1. Prior to the sale, transfer, or other disposal of information resources, the Information Technology Services Department will assess whether to remove data from any associated storage device. (TAC 202.78.b.1)
2. Electronic state records shall be destroyed in accordance with §441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time

the record is removed from data process equipment, the college shall retain a hard copy or other electronic copy of the record for the required retention period. (TAC 202.78.b.2)

3. If it is possible that Category-I/II information resources are contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. (TAC 202.78.b.3)
4. The college shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information: (TAC 202.78.b.4)
   - ❖ date
   - ❖ description of the item(s) and serial number(s)
   - ❖ inventory number(s)
   - ❖ the process and sanitization tools used to remove the data or method of destruction
   - ❖ the name and address of the organization the equipment was transferred to.

5.16.25 Peer-to-Peer (P2P)

Authority-TAC 202.75; Executive Order (RP58)

1. Users of state computers or networks shall not download/install or use any P2P software on state computers, networks, or mobile computing device (PDA) without specific authorization in writing from the IRM. (TAC 202.75.7.V)
2. Any permitted use of P2P software is subject to all information resource policies including the Acceptable Use policy. (TAC 202.75.7.V)

Lamar State College – Port Arthur
Information Technology Services

Policies Revision History

Date	Figure or Section Number	A - Add M - Modify D - Delete	Brief Description
5-10-2011		M	Initial Draft
1-9-2012		M	Policies approved, adopted, and posted.
1-23-13	5.16.1	A	**Added item #9**: It is the responsibility of the Information Technology Services Department to recommend, procure, and maintain all IT hardware and software resources and assets on the Lamar-PA campus in a centrally managed IT organization.
1-23-13	5.16.6	M	**Modified item #2**: **Before:** All production systems must have designated owners and custodians. (TAC 202.71.c) **After:** All production systems must have designated owners and custodians. The Director of Information Technology Services Department shall produce and maintain a Project Management Practices manual. The manual shall contain the methodology for managing information technology projects. The methodology shall include a definition of the varying classifications of projects, and the required components of the methodology for each project classification as required by the Department of Information Resources' Project Management Practices Rule §216. (TAC 202.71.c)