

LAMAR STATE COLLEGE - ORANGE
INSTITUTIONAL PROCEDURES MANUAL
for
INFORMATION RESOURCES

Updated: February 2009

Institutional Procedures Manual for Information Resources

TABLE OF CONTENTS

Forward

I. Information Resources Security

- A. Statement
- B. Purpose
- C. Definitions
- D. Roles and Responsibilities
- E. Specific Responsibilities
- F. Risk Analysis
- G. Personnel Practices
- H. Physical Security
- I. Information Security
- J. Information Systems with Public Access Components
- K. Data Communications Systems
- L. Departmentally Administered Computing Systems

II. Information Resources Support Services

- A. Support Services Statement
- B. DoIT Personnel - General Support Services
- C. DoIT Personnel - Academic/Administrative Support Services
 - 1. Access to Centrally Administered Academic and Administrative Systems/Computers
 - 2. Microcomputer (PC) Support Services
 - 3. Network Procedures & Practices

4. Incident Response Procedure
 5. Academic/Administrative Software Development Support
 6. Data Output
- D. DoIT Security Awareness Program
- E. DoIT Security Risk Assessment and Management Plan

Institutional Procedures Manual for Information Resources

FORWARD

Information resources are the procedures, equipment, facilities, software, and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display or transmit information.

Information resources for the College encompasses the LSC-O Department of Information Technology (DoIT) and the Information Technology Division of Lamar University (ITD of LU). The responsibility for automated data and equipment does not lie solely with the DoIT or ITD of LU. With the advent of distributed processing, responsibility becomes distributed as well. This responsibility is shared by all who are involved with information resources - students, faculty, and staff.

The College's DoIT supports the information resources function and provides computer-related support to all departments of the College and is under the guidance of the Vice President of Academic Affairs.

The College's DoIT is responsible for providing computing services and voice/data communications equipment. The Information technology Division of Lamar University, under the direction of the Associate Vice President of Information Technology Division provide analysis, programming, network and mainframe computer services related to the administrative information systems of the College.

This Institutional Procedures Manual for Information Resources (IPMIR) in conjunction with the Information Resources Security Manual (IRSM) is to be used as a guide for utilizing Information Resources at the College.

I. Information Resources Security

A. Statement

The College is committed to supporting the educational mission of the institution through efficient information storage and retrieval, appropriate auditing procedures, professional personnel services, and a safe environment.

Automated information and information resources residing at the College are strategic and vital assets belonging to the people of Texas. These assets require a degree of protection commensurate with their value.

The protection of assets is a management responsibility which requires the active support and ongoing participation of individuals from all areas and levels of the College. The College community shall take appropriate measures to protect these assets against accidental or unauthorized disclosure, contamination, modification or destruction, as well as to ensure the security, reliability, integrity, and availability of information.

Access to College information resources must be controlled. State law requires that state-owned information resources be used only for official state purposes.

Information which is sensitive or confidential must be protected from unauthorized access or modification. Data which is essential to critical College functions must be protected from loss, contamination, or destruction.

Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value to both the College and potential intruder.

The integrity of data, its source, its destination, and processes applied to it are critical to its value. Changes to data must be made only in authorized and acceptable ways.

In the event a disaster or catastrophe disables information processing and related telecommunication functions, the ability to continue critical College services must be assured.

Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.

Security awareness of employees must be continually emphasized and reinforced at all levels of management. All individuals must be accountable for their actions relating to

information resources.

The College information security program must be responsive and adaptable to changing vulnerabilities and technologies affecting information resources.

The College must ensure adequate separation of functions for tasks that are susceptible to fraudulent or other unauthorized activity.

B. Purpose

The Texas Department of Information Resources requires that an Information Security Function (ISF) be designated to oversee the security of the College's Information Resources. This establishes the Coordinator of Information Resources as the College's Information Security Function (ISF). In its ISF role, the Coordinator of Information Resources promulgates written policies and procedures as necessary to minimize the risk against unauthorized or accidental modification, destruction, contamination or disclosure of information assets, and for the protection of information resources. Information security information is contained in the Information Resources Security Manual, or IRSM.

Texas Administrative Code (1 TAC 201.13(b)) assigns to each head of an agency of state government, the responsibility of assuring an adequate level of security for all data and information technology resources within that agency. The purpose of this IPM for IR is to establish an Information Resources Security Program to:

- a. Assign and maintain management and staff accountability for the protection of information resources.
- b. Promulgate procedures regarding the security of data and information technology resources.
- c. Define minimum security standards for the protection of information resources, including required administrative procedures or management controls.
- d. Provide procedures to assist management and staff in implementing effective security standards and practices where such controls are applicable, as determined by management.
- e. Provide a compilation of information security material in support of security awareness and training programs.
- f. Ensure that security controls do not unnecessarily impede authorized access to information resources.

C. Definitions

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, 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.

Centrally Administered Computer System {WAN, LAN, Lab}

The computing hardware, software, and communications network that comprise any system {WAN, LAN, lab} that is under the direct management of the Computer Center. 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. Included in this definition is the computing infrastructure provided by the campus-wide network and the Computer Center located in the Education and Administration Building.

CIRT

A Computer Incident Response Team (CIRT), is a group of skilled individuals designated by Information Technologies and the Information Technologies Security Committee to respond to any IT incident. Members consist of a combination of Information Technologies personnel and University Police Department personnel.

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 of an Information Resource

The individual responsible for carrying out the function that is supported by the resource, and for defining the degree of access control required by the resource. Custodians are granted custody of specific administrative applications, as well as the data captured, used, derived, and disseminated in those applications.

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 {WAN, LAN, lab} that is under the direct management of any single College organization other than the Computer Center. 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

Unauthorized access to confidential or sensitive information.

Encryption

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

Exposure

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

Information

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

Information Resources

The procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display or transmit information.

Information Security Function (ISF)

The group charged with providing leadership to the College information processing community in the areas of information security, integrity, and privacy. The ISF is comprised of the Coordinator of Information Resources and those who report directly to the Coordinator. The Coordinator may add individuals as necessary to achieve a successful information security program.

IP Address

An Internet Protocol (IP) Address is a unique numerical address that identifies computers connected to the Internet or other IP networks.

IRC

Incident Response Commander -the Information Security Officer (ISO), is the party responsible for managing LSC-O campus-wide IT incident response. Security personnel and Information Technology personnel are eligible to fulfill this role and will be appointed by the President.

IT Incident

An IT incident is any event involving LSC-O information technology resources (whether located at Lamar University or LSC-O) which:

- violates local, state or U.S. federal law, or
- violates regulatory requirements which LSC-O or Lamar University are obligated to honor, or
- violates a LSC-O policy, or

- is determined by the Executive Staff to be harmful to the security and privacy of LSC-O data, IT resources associated with students, faculty, staff and/or the general public, or
- constitutes harassment under applicable law or Lamar University policy, or
- involves the disruption of LSC-O services

IT Resource

All tangible and intangible computing and network assets provided by or for LSC-O in maintenance of its normal operation. Examples of such assets include but are not limited to hardware, software, LSC-O wireless, network access, network bandwidth, mobile/portable devices, electronic information resources, printers, and data.

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.

Owner of an Information Resource

For the purposes of this manual, the owner of information resources is Lamar State College - Orange, a member institution of the Texas State University System, acting on behalf of the people of Texas.

Password

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

Reporter

A person who notifies the ISO of an event believed to be an IT incident.

Risk

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

Risk Analysis

An evaluation of system assets and their vulnerabilities to threats. Risk analysis estimates potential losses that may result from threats.

Risk Management

Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Security Administrator

The individual charged with monitoring and implementing security controls and procedures for a system or administrative application.

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

An event which results in unauthorized access, loss, disclosure, modification, or destruction of information resources whether accidental or deliberate.

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.

User of an Information Resource

Individuals or automated applications that are authorized access to the resource by the custodian, in accordance with the custodian's procedures and rules.

Username

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

Virus

A parasitic program written intentionally to enter a computer without the users permission or knowledge. The word parasitic is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread.

D. Roles and Responsibilities

Information 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 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 - Orange, 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. For the College, the Lamar University Information Technology Division is the predominant agent responsible for the College Administrative Systems (see descriptions in the section on specific responsibilities below), but the College's Department of Information technology, contractors and third party vendors may also perform in 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.

E. Specific Responsibilities

1. College President

It is the President's role to assure that the College's information assets are 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 Coordinator of Information Resources.

2. Lamar University Information Technology Division Personnel

See Information Resource Security Manual filed under Agency 734 for comprehensive details. In general terms Lamar University provides Administrative Information Systems hardware and software support through an interagency contract.

3. Department of Information Technology (DoIT); Lamar State College - Orange

Generally speaking, DoIT, personnel operate in the role of agents for other members of the College community, providing 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 the DoIT are particularly vulnerable to the inadvertent disclosure of confidential or sensitive information.

DoIT 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 Coordinator of Information Resources and the exception 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 DoIT staff. For example, requests for transcript or GPA information should be directed to the Registrar's Office (the designated custodian of official transcript information).

Senior DoIT staff also comprise the Information Security Function (ISF) at the College. These individuals share the ISF responsibilities listed below for centrally administered systems, LANs, labs, and applications. The focus and level (primary, secondary, etc.) of each ISF responsibility will be different for each member of the ISF, 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 serve 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 Coordinator of Information Resources and 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 security 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 through an inter-agency contract by the internal audit department of Lamar University.

- 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.

F. Risk Analysis

Risk analysis is the vehicle for systematically evaluating the vulnerabilities of an information system and its data to the threats facing it in its environment. It is an essential part of any security and risk management program. Absolute security which assures protection against all threats is unachievable. Risk analysis provides a framework for weighing losses which may be expected to occur in the absence of an effective security control, against the costs of implementing the control. Risk management is intended to ensure that reasonable steps have been taken to prevent situations which can interfere with accomplishing the College mission. See specific details related to the LSC-O 'Security Risk Assessment and Management Plan' in section II (E) of this document.

Managers shall periodically complete and/or commission a comprehensive risk analysis of all information resources in their custody. The degree of risk acceptance (i.e. the exposure remaining after implementing appropriate protective measures, if any) must be identified and documented.

The Information Technology Division of Lamar University shall periodically complete and/or commission a risk analysis of information resources considered essential to the College's critical Administrative Information Systems. The Information Technology Division shall prepare and maintain a written and cost-effective Disaster Recovery Plan that provides for the prompt and effective continuation of critical College Administrative Information Systems in the event of a disaster. The Disaster Recovery Plan should be tested and updated periodically to assure that it is valid and remains current.

Data and software essential to the continued operation of critical College functions will be backed up. The security controls over the backup resources will be as stringent as the protection required of the primary resources. Backup of data and software stored on the Lamar University centrally administered computers/servers is the responsibility of the Lamar University Information Technology Division. LSC-O personnel are responsible for making backup copies of data and software used on office computers. These backups can be made using DVD's, CD's, flash drives or requesting network share space for this purpose.

G. Personnel Practices

In any organization, people represent the greatest possible assets in maintaining an active level of security. People also represent the greatest threats to information security; therefore, maintaining employee awareness and motivation is an integral part of the security program.

Managers are responsible for taking any and all measures necessary to insure that departmental staff maintains the confidentiality of information retrieved from the administrative data base. Examples of such information include personnel and payroll records, transcript and grade records, financial aid information, and other sensitive data.

Use of this information for unauthorized purposes is prohibited; as is access to such information in any form whatsoever by unauthorized individuals.

The Coordinator of Information Resources has developed and maintains an Information Resources Security Manual (IRSM) that includes the College's basic security practices. The use of College information resources indicates that the user has knowledge of and agrees to comply with the practices, policies and procedures contained and referenced in the IRSM, IPM for IR and the LSC-O Administrative Policy and Procedures Manual. Managers are responsible for ensuring that all faculty, staff, and student members of their respective departments, including part-time or temporary employees, read and agree to the practices, policies and procedures as outlined in the above mentioned documents.

The DoIT Personnel shall provide literature and/or training at the College's new employee orientation to emphasize security awareness and the importance of individual responsibility with respect to information security. Managers must continually reinforce the value of security consciousness in all employees whose duties bring them into contact with confidential or sensitive information resources.

Managers are responsible for insuring that access privileges are revoked or modified as appropriate for any employee in their charge who is terminating, transferring, and/or changing duties. Managers should provide written notification to the Security Administrator whenever an employee's access privileges should be revoked or changed as a result of the employee's change in status.

The Department of Information Technology shall establish procedures to insure that all security privileges associated with an employee's job function are revoked, once the employee ceases employment with the College. The separating employee shall cease to have any further access to confidential and sensitive information via centrally administered computing resources.

H. Physical Security

All College information processing areas must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations.

Reviews of physical security measures shall be conducted annually by managers, as well as whenever facilities or security procedures are significantly modified.

Physical access to centrally administered computer facilities is restricted to individuals having prior authorization from the Coordinator of Information Resources. Authorized visitors shall be supervised.

The responsibility for securing departmentally-administered computer facilities and/or equipment from unauthorized physical access and/or improper use, ultimately rests with the

manager responsible for the facility and/or equipment.

Employees and information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems. Emergency procedures shall be developed and regularly tested as directed by the College's Office of Risk Management.

Confidential or sensitive information, when handled or processed by workstations, communication switches and network components outside the central computer room, shall receive the level of protection necessary to ensure its integrity and confidentiality. The required protection may be achieved by physical or logical controls, or a mix thereof.

No microcomputer connected to the LSC-O network and/or a currently logged into the Administrative Systems shall be left unattended unless appropriate measures, such as password protected keyboard locking, have been taken to prevent unauthorized use. The owner of the logged-in account is responsible for any activity that occurs under that account.

Physical access to departmentally administered computer facilities, labs and equipment is granted and/or revoked by the administrative head charged with responsibility for the facility and/or equipment. Keys to these facilities should not be issued to any individual without the express permission of the responsible administrative head.

I. Information Security

All information and telecommunication resources leased or owned by the College and all time-sharing services billed to the College shall be used only to conduct official College business except as otherwise provided by state law.

All computer software programs, applications, source code, object code, and documentation are deemed to be a work made for hire and are College property and shall be protected as such if developed either:

- a. by College employees in the course and scope of their employment or with the use of College equipment, materials, or other resources, with the exception of those works covered by a separate intellectual property agreement which addresses ownership rights; or
- b. by contract personnel acting under a contract with the College or the State, unless the contract under which the software or documentation is developed specifically provides otherwise; or
- c. through expenditure of College funds.

All computer software programs, applications, and documentation and associated licenses purchased for use by the College are College property and shall be protected as such.

Confidential information shall be accessible only to personnel who are authorized by the custodian on a strict "need to know" basis in the performance of their duties. Data containing any confidential information shall be readily identifiable and treated as such in its entirety, consistent with College policies and procedures.

When confidential or sensitive information from another College or state agency is received by the College in connection with the transaction of official business, the College shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency or College.

Managers shall specify and/or establish controls to ensure the accuracy and completeness of data and ensure that data comes from the appropriate source for the intended use.

Except for public users of systems where such access is authorized, or for situations where risk analysis demonstrates no need for individual accountability of users, each user of a multiple-user automated system shall be assigned a unique personal identifier or user identification. User identification shall be authenticated before the system may grant that user access to automated information.

A user's access authorization shall be removed from the system when the user's employment is terminated or the user transfers to a position where access to the system is no longer required.

Systems shall implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information they contain and process.

Appropriate audit trails shall be maintained to provide accountability for changes to confidential or sensitive information, software and automated security or access rules.

Controls shall ensure that legitimate users of information resources cannot access stored software or data unless they have been authorized to do so.

Security breaches shall be promptly reported and investigated. If criminal action is suspected, the College must contact the appropriate local law enforcement and investigative authorities immediately.

Test functions shall be kept either physically or logically separate from production functions. Copies of production data shall not be used for testing unless all personnel involved in testing are authorized to access the production data.

Appropriate information security and audit controls shall be incorporated into new systems.

Each phase of systems acquisition shall incorporate corresponding development or assurances of security controls.

After a new system has been placed in operation, all program changes shall be approved by the custodian (or custodian's designee) before implementation.

J. Information Systems with Public Access Components

Information systems with public access components (e.g. self service systems) must incorporate security procedures and controls to ensure data integrity and the protection of confidential information.

Public access systems must authenticate the identity of any individual retrieving, creating, and/or updating sensitive or confidential information about themselves.

K. Data Communication Systems

Network resources participating in the access of confidential information shall assume the confidentiality level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

All network components under College control must be identifiable and restricted to their intended use.

Custodians of distributed information resources served by distributed networks shall prescribe sufficient controls to ensure that access to those resources is restricted to authorized users and uses only. These controls shall selectively limit services based upon:

- a. user identification and authentication (e.g., password, smart card/token), and/or
- b. designation of other users, including the public where authorized, as a class (e.g., public access through dial-up or public switched networks), for the duration of a session, and/or
- c. physical access controls.

Network access to an application containing confidential or sensitive data, and data sharing between applications, shall be as authorized by the application custodians and shall require authentication of any user of the application.

Each College department shall, as part of its contingency plan, provide for an alternate means of accomplishing its program objectives in case the system or its communication network becomes unavailable. Alternative procedures shall be established that enable College personnel to continue critical day-to-day operations in spite of the loss of the communication network.

For services other than those authorized for the public, users of dial-up terminals shall be positively and uniquely identifiable and their identity authenticated to the systems being

accessed.

Communication system identification screens shall include the following warning statements:

- a. Unauthorized Access (Use) is Prohibited
- b. Usage May be Subject to Security Testing and Monitoring
- c. Abuse is Subject to Criminal Prosecution.

L. Departmentally Administered Computing Resources

Departmentally administered computing resources used to store, process and/or access confidential or sensitive data, shall undergo risk analysis. Managers must be prepared to demonstrate that the provisions of this IPMIR have been satisfied for all computing resources for which they are responsible.

II. Information Resources Support Services

A. Support Services Statement

The Department of Information Technology (DoIT) provides information technology related support to all departments of the College and is under the guidance of the Vice President for Academic Affairs.

The DoIT maintains and operates the computer center for both academic and administrative LAN/WAN connectivity, for both voice and data communications. The DoIT is responsible for equipment replacement and repair in both the voice, video and data areas. The DoIT personnel further provide faculty, students, and staff with technical assistance and microcomputer maintenance service.

B. DoIT Personnel General Support Services

1. Planning and Reporting –
The Coordinator of Information Resources acts as the Information Resources Manager for the College and as such is responsible for preparing and sending plans and reports that are required by the Department of Information Resources of the State of Texas.
2. Mainframe Computer Interruptions -
The guidelines pertaining to the mainframe computers are contained in Policy and Procedure Manuals promulgated by the Information Technology Division of Lamar University. Contract Associate Vice-President for Information Technology at 409-880-8493 for specifics.
3. Telecommunications Support -
The DoIT personnel are responsible for the operation of the telephone (voice)

system, data networks and all related equipment on the campus.

4. Access to Centrally Administered Computer Facilities

Only persons designated by the Coordinator of Information Resources, President of the College or Director of Security shall have physical access to centrally administered computer facilities. Included is the Lamar - Orange Computer Center and LAN room, located in the Academic Center Building as well as all rooms containing network equipment. Keys to these facilities will not be issued to any individual without the permission of the Coordinator of Information Resources.

The list of all personnel authorized to enter the Computer Center is as follows:

- (1) College President and Vice Presidents
- (2) DoIT Personnel.
- (3) DoIT Student Assistants.
- (4) Scheduled tours led by the Coordinator of Information Resources.
- (5) Physical Plant personnel delivering items or responding to a call placed by DoIT staff.

Computer Facility Tours

- (1) A tour must be scheduled with the permission of the Coordinator of Information Resources.
- (2) The tour will be guided by a DoIT staff member.
- (3) The maximum allowable number of persons on the tour is five.
- (4) The maximum amount of time the tour members may remain inside the Computer Center facilities is fifteen minutes.
- (5) The tour members will be instructed not to touch anything without specific permission.
- (6) The tour members will be instructed to stay together and not wander away from the group.

All other entries are by special permission of the Coordinator of Information Resources. Any such person entering the Computer Center is to be monitored and any action taken by the person is the responsibility of the person authorizing their entrance. There shall be no extended visits by personnel in this area.

5. Sale, Transfer, or disposal of Information Resources

The sale, transfer, or disposal of old, obsolete, damaged, nonfunctional or otherwise unneeded computers, computer peripherals, and computer software creates information security risks for the College. These risks are related primarily to the information that might be stored on the hard disks and other computer storage media to be included in the disposition. Consequently, only DoIT personnel are to authorized to dispose of information resources equipment. LSC-O departments that have information resources equipment that is to be disposed should complete an

LSC-O DoIT work order request and detail what information resources equipment is to be disposed of.

C. DoIT Personnel Academic/Administrative Support Services

1. Access to Centrally Administered Academic and Administrative Systems/Computers

a. Student - User ID's

Student accounts are automatically generated and the student's userid and passwords are accessed by each student through the use of the student administrative self-service application (by accessing the student login link located on the MyLSC-O homepage). The userids are generally created using an algorithm that follows the student's first initial, middle initial and last name (up to 10 character; with numbers being substituted in the cases of duplicates). In the absence of any initial(s), that letter is skipped.

b. Faculty/Staff - User ID's

Faculty/Staff accounts are requested by using an Information Resources Request form, which is contained as part of the initial hiring packet for new employees. The form should be completed, signed, and included with all other hiring packet information necessary in the hiring process. The Human Resources Office will generate the creation of the account username by placing a PIN number on screen WEB in the HRS system. The Information Resources Request form is signed by the HR staff member following the entry of the PIN number. The form is then routed to the DoIT personnel for completion of Information Resources access and Administrative System access if requested.

Administrative system accounts are added by the Campus Security Officer(s). These administrative accounts are captive accounts and have no access to a dollar prompt. Disk space and a log-in directory are created for a user by the Campus Security Officer(s) through a self service system generated by the systems personnel of the Information Technology Division of Lamar University.

Administrative System Access Acquisition Procedures:

- (1) Information Resources Request form with Administrative System access requested is forwarded by the DoIT personnel to appropriate data custodian for appropriate screen access list and approvals.
- (2) Campus Security Officer creates Administrative account with access that is detailed on completed forms returned by the appropriate data custodian.

(3) Campus Security Officer completes notification memo and mails to requesting faculty/staff member.

(4) All forms are filed and retained by the DoIT.

c. User Passwords

Academic and administrative users are issued a password for each separate information resources accessed. Refer to the Lamar University Information Resources security Manual (section III, B, 3) details concerning the criteria related to the Administrative System password. Refer to the LSC-O password policy contained in section 5.11 of the LSC-O Administrative Policy and Procedures Manual for details concerning the criteria related to the LSC-O network account/password.

2. DoIT Personnel Microcomputer Support Services

a. Help Desk

For campus information resources work orders, the requestor can fill out the web based computer work request form or call the Switchboard personnel to generate a work order.

The switchboard is attended by the switchboard operator or student assistants.

(1) User calls the switchboard at extension 0.

(2) If possible, Operator will resolve problem and proceed to Step 6.

(3) The request is logged, assigned a number, functional area, and priority.

(4) The request is forwarded to the appropriate support person.

(5) The User is contacted, resolution is reached.

(6) Call is closed.

b. Hardware/Software Procurement Services provided:

Computer hardware and software procurement at the College represents a significant investment. This investment must be effectively planned, utilized, and managed. This acquisition procedure is a step toward proper management and control of this vital resource.

All computer related acquisitions (exclusive supplies) are to be sent to the Coordinator of Information Resources. A check will be run for similar acquisitions in order to get volume buying and will comment on whether the acquisition will be supported by their group. This process should add no more than three (3) days to the requisition process and will provide users with better prices and maintainability on the chosen system. The routing document is signed by the Coordinator of Information Resource and returned to the Department for proper signatures. The Department will then forward

the routing document and requisition to Purchasing for processing.

When a Department is not familiar with computer equipment or is not aware of what is offered or how to configure what they need, they should contact the Coordinator of Information Resources for assistance. They can provide recommendations and advice along with vendor comparisons and can advise on network setup and installation. In order to avoid waste caused by duplication of facilities and effort, anyone considering computer-related acquisitions should utilize this group for assistance in their planning and procurement.

c. Hardware Life Cycle & Support

The Academic computer labs have a life cycle of three (3) years. At the end of the three year cycle the PC's will be evaluated for continued lab use based on hardware/software minimums needed for academic uses. Microcomputers are removed to faculty/staff offices if unable to perform necessary lab functions.

The DoIT personnel work in conjunction with the Purchasing Office to ensure that the College receives the best quality computer equipment as well as the best economic value. The DoIT personnel will support microcomputers and printers based on the following guidelines:

The following personal computers will be supported:

-Pentium or new model processor

Upgrades

The DoIT personnel provide assistance when upgrading microcomputers, hard drives, memory, and other boards and peripheral equipment.

Payments for upgrade components are provided by the DoIT, if funds are available and upgrade is recommended.

Laser Printers

The DoIT will provide installation and pickup services related to printer repairs. Laser printers will be repaired off-site. The cost of repairs will be the responsibility of the requesting department. Laser printer cartridges are provided by the DoIT, if funds are available.

Due to the rapid changes in technology, the type of hardware supported is subject to change. The DoIT continuously evaluates and monitors microcomputers and peripherals. Evaluation/monitoring results may cause a change in the list of supported hardware. Improvement or changes in

functionality, compatibility, reliability and campus needs may also result in items being added or removed from the list of supported hardware.

d. Software

The DoIT supports a variety of commercial software packages for the College. Support is provided for the version considered to be the standard for the College. The major categories of supported software include Word processing, Spreadsheets, Database, Terminal Emulation/Communications, Operating Systems, Network Operating Systems, Graphics and E-Mail.

The DoIT may not support Freeware, Shareware, or Public Domain software. Freeware refers to software that has a copyright and is available at no charge. Public domain software does not have a copyright and can be distributed without obtaining permission or paying a fee. Shareware is software that is available on a trial basis; if a shareware program is used permanently, then a fee is expected to be paid to the author.

The DoIT personnel are familiar with a core set of software and can only provide support for those applications. The DoIT personnel will help install licensed non-supported software, but are not in a position to troubleshoot problems associated with the use of the software.

There shall be no loading of personal software on College computers any such software found will be removed.

The DoIT personnel will not install software on faculty or staff personally owned computers.

The DoIT personnel will not support, nor install, pirated software.

The installation of any software package and/or data files on individual faculty/staff PC's must be approved by the Coordinator of Information Resources. The installation of any software will be performed by DoIT personnel.

DoIT personnel will support software as follows:

Microsoft Networks

PC Application Software

- Microsoft Office Components
- NetScape
- Internet Explorer
- Adobe Acrobat Reader

Operating Systems

- Microsoft Windows XP

E-Mail Applications

- Microsoft Outlook Web Access
- MyLSC-O

Anti-Virus Software

3. Network Procedures & Practices

a. Backups

The LSC-O network servers are backed up to a 3 terabyte SAN storage device and an LTO-3 tape autoloader. Full backups of each server are performed each night to the SAN. The SAN then backs up to the tape system every day. Tapes are rotated off-campus to the safety deposit box at Capital One bank on a regular basis. The only exception to this procedure is the Pharmacy server. The reason for this is because the server contains no confidential or security sensitive data, only the applications used by the Pharmacy program. Whenever the software on the server is updated, a full system backup is performed. The hard drive is also imaged using Ghost at least once each full semester for additional redundancy.

b. Disaster Recovery & Business Continuity

Lamar University is paid through an inter-agency contract for administrative computer resources. The Lamar University - Information Technology Division is responsible for developing and maintaining a Disaster Recovery Plan designed to address the operational restoration of Lamar State College - Orange's critical administrative computer processing capability. This plan should identify the strategy to recover centrally administered data storage, programs, and processing capability in the event that the Lamar University Computer Center in the Cherry Engineering Building is rendered inoperable. The plan should also include 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 Disaster Recovery Plan referenced above does not address the needs of individual operating units beyond the restoration of access to their critical centrally administered applications. All College departments are required as part of the College budget cycle to present updated Emergency Management

Plans for business operations during an emergency. These local service disruption plans should address losses ranging from minor temporary outages to catastrophic losses.

For the details concerning the College Information Resources Disaster Recovery Plans refer to the LSC-O Emergency Management Plans related to the Telecommunications Unit and the Computer Center Unit. These plans do not address relocating the academic computer labs used for instructional purposes. The computer labs will remain on-site and the situation monitored daily.

c. Management & Configuration

Lamar State College - Orange Department of Information Technology, under the direction of the CIO, has responsibility for management and security of the Lamar State College - Orange (LSC-O) Network.

(1) Technology Support Personnel

- All technical support positions, regardless of departmental and divisional reporting authority or funding, are classified as security sensitive and require human resource approved background checks prior to extending any invitation for an interview. Included are those positions that support faculty, staff and student computing and instructional technology resources.
- All technical support positions regardless of departmental and divisional reporting authority or funding shall be required to attend an annual briefing on information security as well as emergency briefings as determined by the CIO.

(2) Addressing and Domain Services

- Individuals, grant offices, academic departments or administrative departments at LSC-O may not create nor support an Internet domain, hosted from the LSC-O's network without prior approval of the Executive Staff Committee.
- The LSC-O network and security administrator(s) will administer the LSC-O IP address space, all network protocols and the lsc.edu domain. The Department of Information Technology will manage any additional domains approved by the Executive Staff Committee.

- Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to computers. The LSC-O network and security administrator(s) will give prior notice to affected users before making any changes.

(3) Network Connections

- LSC-O departments, faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system which requires physical attachment to the LSC-O network without the prior review and approval of the CIO or designee. Wireless connectivity is provided in some areas but requires a valid LSC-O network account for access. All wireless connectivity must be configured using WEP and 802.11 standards.
- All wired devices placed on the LSC-O network must be registered and assigned a physical network port with the network and security administrator(s). Devices may not be moved to a new port without approval and assistance of the LSC-O Computer Center staff.
- Physical access to LSC-O networking equipment (servers, routers, switches, etc.) is not permitted without the prior approval of the CIO or designee.

(4) Firewall & Port Security

- The LSC-O network and security administrator(s) will take action to prevent source network address forgery (spoofing) of internal network addresses from the Internet and will also take action to protect external Internet sites from source address forgery from the LSC-O's network.
- The LSC-O's external Internet firewall practice is to deny all external Internet traffic to the LSC-O's network unless explicitly permitted. Access and service restrictions may be enforced by IP address and/or port number. Proxy services may be used in conjunction with the firewall to restrict usage to authenticated individuals. This practice is designed to protect LSC-O network users from attacks launched from the Internet.
- LSC-O must identify systems that will offer Internet services, to better protect them. To facilitate this, academic and administrative departments must register with the CIO or designee, systems that

require access from the Internet. These systems must also be protected by access control software.

- The LSC-O's internal Internet firewall practice is to allow all internal IP traffic outbound to the Internet unless explicitly denied. This practice may be changed in the future if the situation warrants it.
- Some network services through standard ports are supported. However, services may be restricted to a limited number of subnets or hosts. For example, electronic mail may only be sent and received by authorized mail servers on campus. User access to the mail accounts on these servers will be permitted from off-campus through the firewall.
- Most network services through non-standard ports are not supported. Services through non-standard ports may be restricted to a limited number of subnets or hosts. For example, WWW access via the standard HTTP port (Port 80) will be permitted, but to some other arbitrary port number may not be permitted.
- Limited encrypted tunnels for passing through the firewall to internal resources, such as X-Windows, is permitted with the prior approval of the CIO or designee. The recommended method is to use Secure Shell (SSH). IP Multicast tunneling is not permitted.
- All modem connections that allow someone from outside to access to the LSC-O's network must be registered with the CIO or designee. The LSC-O reserves the right to block any modem connections, or disconnect any computer system, that allows unauthorized access to the network.

(5) Network Security

- The CIO or designee shall identify the appropriate network security level for LSC-O systems, in collaboration with academic and administrative departments. These levels should be divided into the following categories, from highest to lowest: Mission-critical, Important, and Normal. Efforts shall be made to protect these systems at the appropriate level. The CIO or designee will determine the security status of LSC-O computer systems and review it periodically.
- The CIO or designee will investigate any unauthorized access of LSC-O computer systems. Through the direction of Executive Staff

Committee, the CIO or designee will work with administrative departments, system counsel and/or law enforcement when appropriate.

- Systems on the network must have adequate security installed and maintained. All systems connecting to the LSC-O network must be configured and maintained in such a manner as to prohibit unauthorized access or misuse.
- If security problems are observed, it is the responsibility of all LSC-O network users to report problems to the appropriate system administrators or the CIO or designee for investigation.
- Network usage judged appropriate by the LSC-O is permitted. Some activities deemed inappropriate include, but are not limited to:
 - Establishing unauthorized network devices, including router, gateway or remote dial-in access server or a computer set up to act like such a device.
 - Engaging in network packet sniffing or snooping.
 - Operating network servers of any sort in violation of LSC-O guidelines.
 - Setting up a system to appear like another authorized system on the network (Trojan).
 - Other unauthorized use prohibited by the LSC-O's acceptable use or other policies.

(6) Emergency Maintenance Authorization

- Recognizing the immediacy required to respond to security breaches or published security vulnerabilities, the LSC-O network and security administrator(s) is authorized to remove any server from operation at anytime for the purpose of installing security patches; updating virus protection software; and/or for securing forensic evidence of intrusion.
- Users are responsible for taking immediate action to email and voice mail broadcasts disseminating information pertaining to emergency security updates required for workstations and/or servers within their control and/or assigned job responsibilities.

(7) Monitoring and Auditing

- The network and security administrator(s) will maintain traffic logs of the firewall for security auditing purposes based upon retention schedules set by the CIO or designee.
- Through the direction of Executive Staff, the CIO or designee reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a LSC-O policy violation. Reasonable cause may be provided by a complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of the staff.
- With permission from the CIO or by order of the Executive Staff, DoIT personnel staff may perform a security audit of any computer system attached to the network. The CIO will provide the report to the Executive Staff at the completion of the audit.

(8) Enforcement and Recourse

- The LSC-O Administration considers any violation of acceptable use principles or guidelines to be a serious offense, and reserves the right to test and monitor security, including copying and examining any files or information resident on LSC-O computer systems allegedly related to unacceptable use. (See Information Resources Acceptable Use Policy; See also TSUS Appropriate Use Policy [pending approval])
- Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network in any way is subject to immediate disconnection from the LSC-O's network. The CIO or designee may require specific security improvements where potential security problems are identified.
- Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. This includes but is not limited to attaching unregistered devices to the network; sharing passwords; leaving systems unattended that are logged into security sensitive servers; unauthorized monitoring of the network; and assisting someone else or requesting someone else to circumvent security or administrative access controls.
- Persons responsible for policy violations are subject to action in accordance with student, faculty and staff disciplinary policies and procedures and possible prosecution from local, State or Federal

authorities.

(9) Server Hardening

The Microsoft Windows Server Update Services (WSUS) are currently in use at LSC-O. The current version in use is WSUS-3. This service provides Microsoft updates, both application and operating system, for both PC's and servers on campus. All PC's on campus are grouped in either the lab group or the faculty/staff group. The patches related to PC's are updated automatically for those PC's in the faculty/staff group. Those PC's in the lab group are not updated since LSC-O uses an application called Deep Freeze which secures the PC OS from modification.

The server critical patches are downloaded automatically and applied to all servers. The lesser classification of patches are reviewed prior to installation.

4. Incident Response Procedure

a. Reason for this Procedure

The College's Department of Information Technology may at times be required to work with law enforcement, either internal (Security Department) or external, in the reporting of and responding to information technology incidents/threats. Such response is necessary to ensure the secure operation of the College's Information Technology assets, to protect the data security and privacy of students, faculty, and staff, and address appropriately to DIR and/or federal requirements.

b. Statement of Procedure

(1). Incident Classification - To help facilitate accurate and productive responses to IT incidents, the ISO will classify and assess all IT incidents for severity at soon as they are recognized. The classification may be altered as the IT incident progresses, and therefore the ISO should re-evaluate the situation periodically. When an IT incident falls under more than one classification, the classification of highest severity should guide the course of the IT incident response. The ISO is responsible for providing and maintaining appropriate IT incident classification guidelines and resolution procedures.

(2). Reporting - The ISO is responsible for determining whether a reported event is an IT incident following receipt and evaluation of the report. Upon

receiving a report, the ISO should assess its veracity, determine if it is indeed an IT incident, classify it, and initiate handling procedures.

Whenever an observed event appears to satisfy the definition of an IT incident, it should immediately be reported to the ISO, who will relay the report to the ISO. Events whose classification is questionable should still be reported to the ISO for evaluation. All available, relevant information about the event should be reported, including but not limited to dates, times, persons/resources involved, and IP addresses. The ISO is responsible for publishing all IT incident reporting guidelines and additional contact information. Suspect events also may be reported to the ISO via email to Linda.Burnett@lsc.edu.

Incident reporting as described in this procedure does not replace law enforcement notification in the event of a suspected illegal action. All suspected criminal events should be reported immediately to an appropriate law enforcement agency. Should an event possibly be both a crime and an IT incident, it should first be reported to law enforcement, and then notification that a police report has been filed should be sent to the ISO.

The College faculty, staff, and students should report crimes to the Director of Security at 409-882-3910. All persons external to the college should report crimes to their local law enforcement agency.

(3). Response - After receiving a report, assessing its veracity, determining whether or not the event constitutes an IT incident, and if so, classifying the IT incident, the ISO or his/her designee will determine if the incident warrants a formal response. IT incidents that do not warrant a formal response as determined by ISO and Executive Staff will be remanded to the SC for closure. Actions taken with respect to all reported events and IT incidents must be documented throughout the response process.

If the ISO, or other, appropriate designated personnel, determine that an event requires a formal IT incident response, it is the responsibility of the ISO to coordinate the appropriate resources for that response. If appropriate, a CIRT will be formed and assigned to the IT incident. The CIRT will be led by an IT or Security representative appointed by the ISO.

The ISO (or an appropriate designee) is responsible for documenting appropriate procedures for responding to event reports and IT incidents, and for coordinating CIRTs.

(4). Business Continuity - Under some circumstances, an IT incident may

require -- subject to applicable laws and College policies -- the suspension of involved or targeted services/systems in order to:

- Protect students, faculty, staff, IT resources, other systems, data, and/or College assets from threats posed by the involved services/systems
- Protect the service/system in question
- Preserve evidence and facilitate the IT incident response process

The decision to suspend operations will be made by the ISO. In the case of mission-critical applications, the ISO will make a good-faith effort to consult with the appropriate SC and, if available, the service/application owners before such suspensions are implemented. If, in the sole judgment of the ISO, an excessive amount of time (giving due consideration to the relative severity of the IT incident) has passed without response from the appropriate SC or service/application owner, suspension may occur without consultation.

Any non-college equipment which is using College IT resources and is found to be the target, source, or party to an IT incident may be subject to immediate suspension of services without notice until the issue has been resolved. This includes, but is not limited to, network access for student residents and contractor equipment. It is the ISO who shall determine whether a service suspension may be lifted.

In order to facilitate proper and timely handling of IT incident responses, it is essential that network-connected devices can be identified and located in a timely manner. To this end, SCs are required to maintain an inventory of network-connectable devices under their control, in conformance with guidelines established by the ISO. Absent such guidelines, SCs are required to maintain a list of all such devices including, at a minimum, the primary location of each device, and the physical address (MAC address) for all network interfaces used by it.

(5). Scope - This procedure covers students, faculty, staff, and all other individuals or entities using College IT resources as well as all uses of such IT resources. By using College IT resources an individual or entity consents to all of the provisions of this policy document and agrees to comply with all of the terms and conditions set forth herein, all other applicable College policies, regulations, procedures and rules, and with applicable local, state and federal law and regulations.

Violations of this policy may result in the revocation or limitation of IT

resource privileges as well as administration of other disciplinary actions, and may be referred to appropriate external authorities.

(6). Related Documents - Laws that influence and affect this policy Include but are not limited to:

COPPA <http://www.ftc.gov/coppa/>

DMCA <http://www.copyright.gov/legislation/dmca.pdf>

ECPA

<http://www.access.gpo.gov/uscode/title18/part1 chapter119 .html>

FERPA <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

GLBA <http://www.ftc.gov/privacy/glbact/>

HIPAA <http://www.hhs.gov/ocr/hipaa/>

USA Patriot Act <http://www.lifeandliberty.gov/>

Lamar University and Texas State University System Acceptable Use Policy (currently under development).

(7). Contacts - For questions concerning this procedure contact the ISO at Linda.Burnett@lsc.edu

(8). Dissemination - As required elsewhere in this procedure, the ISO (or designated representative) is responsible for publishing all guidelines for reporting, classifying, responding to, and communication of IT incidents.

(9). Compliance- Failure to comply with this procedure may result in disciplinary or administrative action, to include temporary or permanent loss of IT resource privileges or services.

5. Academic/Administrative Software Development Support

a. Overview

The Information Technology Division of Lamar University; Administrative Systems department provides systems analysis and programming services for the administrative systems. College employees requiring information from an administrative database should contact the official custodian of the data for authorization. A custodian is the person responsible for the function supported by the data and is usually easy to identify (i.e., Financial Data-VP for Finance; Student Data-VP for Student Services; Human Resources Data-Director of Human Resources). If programming is required, requests for systems development should be made following the System Development Life Cycle promulgated by the Information Technology Division of Lamar University.

b. Ownership

Software Ownership

- (1) All programming software, developed during working hours by persons working for the College, is the exclusive property of

- the College.
- (2) All software purchased by the College is the exclusive property of the College to the full extent allowed by the vendor license agreement.
 - (3) Purchased software and software documentation are copied only as allowed by law and the license agreement with the vendor of such software.
 - (4) Personnel may not purchase or write their own software for use in the organization without authorization.

Data Ownership

- (1) Data files developed by the user's department are the property of that department and will be kept in an academic computer account under a department userid, or on a department computer.
- (2) Data files developed by the Lamar University - Information Systems for the College are the property of the College.

6. Administrative Information System Data Output

Administrative system reports are directed to LSC-O network printers located and under the physical control of the Business Office.

These reports are then dispatched by the controlling department to the individual noted on the face of the report or brought to the mailroom for dissemination to the noted faculty or staff member.

D. DoIT Security Awareness Program

The Security Awareness Program at LSC-O has been developed with repetition in mind. The more times that individuals are exposed to information the more likely they are to absorb the information.

The Security Awareness Program at LSC-O is comprised of the following activities:

- Emailing of DIR Cyber Security newsletters to campus community
- Emailing of current SPAM notifications to campus community
- DoIT sponsors a booth at yearly Spring Day event. The DoIT personnel set up a technology booth that is visited by students, faculty and staff.
- Yearly briefing of security concerns occur at the:
 - Fall Faculty Convocation
 - Fall Staff Convocation

- Security practices monitoring
 - DoIT personnel walk around the campus and if they see an unoccupied faculty and/or staff PC the PC is checked to see if the PC has been locked. A security token is left at PC based on what is found. A 'Good Practices' or 'Bad Practices' token is left on the keyboard based on the locked or unlocked condition of the PC.

E DoIT Security Risk Assessment and Management Plan

The data that has been ranked as high risk and medium risk and that is stored on the LSC-O administrative systems which are located on the mainframe computer located at Lamar University. It is the responsibility of Lamar University to protect the data through the application of the Lamar University Policies, Procedures and Risk Management Plan. The secondary high risk and medium risk factors associated with individuals being granted access to the data contained in these systems is mitigated through the administrative computer account process.

The data that has been ranked as high or medium risk and is located in the LSC-O Computer Center is assessed on an annual basis through the use of the ISAAC tool (Information **S**ecurity **A**ssessment, **A**wareness, and **C**ompliance) provided by the Department of Information Resources and the University of Texas.

To further mitigate risks the following practices are followed at LSC-O:

- Active Directory accounts are created as power users only (not administrators). This reduces the risk of non-LSC-O software being loaded on LSC-O PC's. If non-administrators try to load software an error message is generated.
- PC's located in labs both open and those designated for classroom use are protected from alteration through the use of system consistency software (Deep Freeze). Each time the PC is booted the PC will revert back to the LSC-O image originally installed.
- Automatic OS updates to faculty/staff PC's guard against attacks using known OS vulnerabilities.
- Automatic OS updates to servers guard against attacks using known OS vulnerabilities.
- Hourly virus definition file checking is configured for each faculty/staff PC
- Hourly virus definition file checking is configured for the server controlling the virus file definition that is accessed by faculty/staff PC's.

- All non-essential ports to servers are disabled.

For the protection of all Information Resources Lamar State College – Orange has the responsibility of adhering to the policies and procedures detailed within this document, and the LSC-O Policies and Procedure manual and the LSC-O Information Resources Security Manual.

Both this document and the LSC-O Information Resources Security Manual are reviewed at least annually and/or updated to reflect additional/updated guidelines as necessary. The LSC-O Emergency Management Plans for the Telecommunications and Computer Center units are updated at least annually during the budget cycle or as necessary based on changes within the LSC-O Information Resources environment.