

LAMAR STATE COLLEGE - ORANGE
INFORMATION RESOURCES SECURITY MANUAL
for
INFORMATION RESOURCES

Updated: June 2007

Information Resources Security Manual

- 1. Purpose of Security Manual**
- 2. Audience**
- 3. Acceptable Use**
- 4. Account Management**
- 5. Administrative/Special Access**
- 6. Backups**
- 7. Change Management**
- 8. Computer Virus Prevention**
- 9. E-mail**
- 10. Incident Management**
- 11. Incidental Use**
- 12. Internet Use**
- 13. Information Services Privacy**
- 14. Network Access**
- 15. Network Configuration**
- 16. Passwords**
- 17. Physical Access**
- 18. Portable Computing and Remote Access**
- 19. Security Monitoring**
- 20. Computer Security Awareness/Training**
- 21. Operating System Hardening**
- 22. Software Licensing**
- 23. Enterprise Development and Deployment**
- 24. Vendor Access**
- 25. Disciplinary Actions**
- 26. Supporting Documentation**

1. Purpose of Security Manual

The purpose of this manual is to establish a College-wide approach for the consistent handling and control of all College Information Resources with respect to security, access and confidentiality. This manual also provides direction and defines procedures relating to the operational implementation of the LSC-O Institutional Procedures Manual for Information Resources.

2. Audience

The Lamar State College - Orange Information Resources Security Manual provides guidance for all individuals that have, or may require, access to Lamar State College - Orange Information Resources.

3. Acceptable Use

Before an individual is provided access to a Lamar State College – Orange technology resource he or she must acknowledge the Lamar State College – Orange, Information Resources Use policy, the Lamar State College – Orange, Information Resources Security Manual and the Lamar State College – Orange, Institutional Procedures Manual for Information Resources (IPMforIR). This acknowledgement is contained on the Information Resources Request Form.

4. Account Management

The following account management practices are required:

- All accounts that access non-public Lamar State College – Orange Information Resources must follow an account creation process. This process should document who is associated with the account, the purpose the account was created for, and who approved the creation of the account. All accounts wishing to access non-public college Information Resources must have the approval of the owner of these resources.
- Accounts of individuals who have had their status, roles, or affiliation with the college change must be updated to reflect their current status.
- Password aging and expiration dates must be enabled, where supported by the underlying account mechanism, on all accounts created for outside vendors, external contractors, or those with contractually limited access to the college's information resources.

5. Administrative/Special Access

Users must be made aware of the privileges granted to their accounts, especially those that could impact access to Information Resources or that allow them to circumvent controls in order to administer the information resource. Abuse of such privileges will not be tolerated. Anyone using accounts with privileges of this type must adhere to the following access requirements.

- Individuals that use accounts with special privileges must use these accounts only for their intended administrative purposes.
- Individuals that use accounts with special privileges may perform investigations relating to potential misuse of Information Resources by an individual user only under the direction of the Information Security Office.
- The password for a shared administrator/special access account must change when any individual knowing the password leaves the department or Lamar State College - Orange, or changes role, or upon a change in the vendor personnel assigned to the Lamar State College - Orange contracts.

6. Backups

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

7. Change Management

The Information Resources infrastructure at Lamar State College - Orange is constantly changing and evolving to support the mission of the organization and its departments. Computer networks, servers, and applications require planned outages for upgrades, maintenance, and fine-tuning. The following change management procedures are required in proportion to the respective data classification category, the availability requirements of the data, and the impact of the change on the user community:

- All changes to environmental controls affecting computing facility machine rooms (for example, air-conditioning, water, heat, plumbing, electricity, and alarms) should be reported to the Department of Information Technology.
- Departments or entities responsible for Information Resources will ensure that the change management procedures and processes they have approved are being performed.
- A department or entity may object to a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out contingencies, inopportune timing in terms of impact on service to users or in relation to key business processes such as year end accounting, or lack of resources to address potential problems that may be caused by the change. All objections will be reviewed by the responsible department or entity.
- Whenever possible, customers will be notified of changes following the steps contained in change management procedures.
- For the administrative information systems located on at Lamar University the tracking of changes follows the process described in the System Development Life Cycle document. Change management tracking data should contain at least the following information:
 - Date of submission and date of change
 - Owner and custodian contact information
 - Nature of the change

8. Computer Virus Prevention

A variety of technologies and practices are required to protect the Lamar State College – Orange network infrastructure and other Information Resources from threats posed by computer viruses, worms, and other types of hostile computer programs.

- The Lamar State College – Orange department of Information Technology installs current virus protection software on all Lamar State College - Orange computers and servers on the college network.
- E-mail gateways must utilize properly maintained e-mail virus protection software.
- Any computer identified as a security risk due to lack of virus protection may be disconnected from the network or the respective network access account may be disabled until adequate protection is in place.
- Every instance of a computer virus infection constitutes a security incident and must be reported to the Department of Information Technology.

9. E-mail

Electronic mail (E-mail) is an essential tool for communicating within the college. It is important that unimpeded e-mail services be available at all times and that e-mail be used in a manner that achieves its purpose without exposing the college to unnecessary technical, financial, or legal risks. The following practices are required:

- All e-mail is subject to logging and review.

- To reduce spam and protect the e-mail environment from malicious viruses, worm or other threats, the Department of Information Technology, or an otherwise appropriate department or entity, may filter, block, and/or strip potentially harmful code from messages.

10. Incident Management

Incident management is needed to assure continued operations in the event of a security breach or incident involving a computer virus, worm, attack against college information systems, or misuse of Information Resources. The Department of Information Technology is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operation quickly and if required, maintains evidence for further disciplinary, legal, or law enforcement actions.

11. Incidental Use

Incidental personal use by Lamar State College - Orange affiliates of Information Resources is permitted per the Information Resources Use Policy. The Department of Information Technology or the appropriate department or entity is permitted to monitor the incidental personal use of Information Resources to ensure that:

- Use is restricted to Lamar State College - Orange affiliates only.
- Use does not result in a direct cost to Lamar State College - Orange.
- Use does not expose the college to unnecessary risks.

12. Internet Use

The Lamar State College - Orange network users must adhere to prudent and responsible Internet practices to mitigate risks associated with the Internet. The following practices are required:

- Software and operating systems utilizing the college network are expected to be kept updated and to have features that enhance network security enabled.
- Content on all Lamar State College - Orange departmental web sites must relate to college business, service, and/or academics and must be approved by the appropriate department or entity publishing the information.
- Purchases for Lamar State College - Orange handled via the Internet are subject to the appropriate Lamar State College - Orange procurement rules.
- Personal commercial advertising must not be posted on Lamar State College - Orange web sites.

13. Information Services Privacy

The Lamar State College - Orange may log, review, and otherwise utilize any information stored on or passing through its information resource systems in accordance with the provisions and safeguards provided in the **Texas Administrative Code 202.1-8**, Information Resource Standards.

In cases of suspected abuse of Information Resources, the contents of any e-mail or file may be reviewed in accordance with provisions defined in the Disciplinary Actions section of this manual.

Access to data and information associated with such actions will be handled using standards of privacy and confidentiality required by law and college policy.

14. Network Access

Access to the network is managed to ensure the reliability of the network and the integrity and appropriate use of information contained within the network: The following network access procedures are required:

- No network hardware (router, switch, hub, firewall, wireless access point, or other network appliance) may be installed on the Lamar State College - Orange network without prior notification by the Department of Information Technology.
- Systems attaching to the college network must operate in a way that poses no internal or external security or operational hazard. Owners of systems that do not meet these criteria must cooperate fully with college staff in correcting the problems.

15. Network Configuration

The Department of Information Technology:

- Will operate and maintain a reliable network with appropriate redundancies to meet quality of service goals.
- All registered hosts attached to the college network may be scanned by the Department of Information Technology for potential vulnerabilities.
- Must install or authorize a contractor to install all cabling and network hardware.
- Will approve the specification used to configure all equipment connected to the Lamar State College - Orange network.
- Has the authority over changes to the configuration of active network management devices.
- Sets all protocols and standards used on the Lamar State College – Orange network.
- Must install, configure, and maintain the Lamar State College – Orange network firewalls.
- Provides written authorization for the use of departmental firewalls. Their use is not permitted without written authorization.

16. Passwords & Computing Devices

Strong passwords are required on Lamar State College - Orange accounts. All passwords must be constructed, implemented, and maintained according to the Lamar State College – Orange Password Policy.

Unattended computing devices must be secured from unauthorized access. Physical security options include barriers such as locked doors or security cables. Logical security options include locking desktops and automatic session time-outs.

17. Physical Access

The granting, controlling, and monitoring of physical access is an important component of the overall security program:

- All information technology resource facilities must be physically protected in proportion to the criticality, confidentiality, or importance of their function at Lamar State College - Orange.
- All Information Resources facilities must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.
- Access to information technology resource facilities will only be granted to authorized personnel of Lamar State College - Orange and other contractors or personnel whose job responsibilities require such action.
- Access fobs and/or keys must not be shared or loaned to others.
- Access fobs, and/or keys, that are no longer required must be returned to the responsible department contact. All returned access fobs must be forwarded to the responsible campus

key management center contact as soon as possible. Fobs and/or keys must not be reallocated to another individual, thereby bypassing the return process.

- Lost or stolen access fobs and/or keys must be reported to the appropriate department or entity as soon as possible.
- Visitors must be escorted in controlled areas of Information Resources facilities.
- The appropriate department or entity or a designee must review access records for secured information technology resource facilities on a periodic basis and investigate any unusual access.
- The appropriate department or entity or a designee must review fob and/or key access rights for secured information technology resource facilities on a periodic basis and remove access for individuals that no longer require access.

18. Portable Computing and Remote Access

Computers and devices used to access Lamar State College - Orange infrastructure must do so in a manner that preserves the integrity, availability, and confidentiality of the Lamar State College - Orange information.

19. Security Monitoring

Security monitoring is used for confirming security practices and controls in place are being adhered to and are effective. It is also used in identifying anomalous activity that might be an indication of an operation or security concern. Monitoring consists of activities such as automated notification of security breaches and automated or manual examination of logs, controls, procedures and data. The following monitoring requirements apply to Information Resources at Lamar State College - Orange:

- Operating system user accounting and application software audit logging processes will be enabled on host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control systems must be enabled.
- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and automated tools will report exceptions to the extent technically feasible.
- Information Resources connected to the college network are subject to automated monitoring and notifications of possible security events of interest by the Department of Information Technology.

20. Computer Security Training

The Department of Information Technology is charged with providing a combination of general computer security awareness practices and training.

- All users of the Lamar State College - Orange Information Resources will be provided with training and supporting materials to allow them to properly protect the Information Resources they use.
- Security awareness practices will be disseminated by the Department of Information Technology.

The Department of Information Technology

- Must prepare, maintain, and distribute information that concisely describes the Lamar State College - Orange Information security policies and procedures.

- Must develop and maintain a process to communicate new computer security program information, security bulletin information, and security items of interest to faculty, staff and students.
- Will provide specific security training to information technology professionals serving in positions of special trust (for example, system administrators).

21. Operating System Hardening

Information and services must be transmitted securely and reliably to assure that data integrity, confidentiality, and availability are preserved. To achieve these goals, systems must be installed and maintained in a manner that minimizes service disruptions and prevents unauthorized access or use. The following standards apply:

- A system must not be connected to the Lamar State College - Orange network until it is in a secured state and location (as defined by the responsible department or entity).
- The following general steps are:
 - Installation of the operating system from a reliable source.
 - Application of vendor supplied patches.
 - Removal of unnecessary software, system services, and drivers.
 - Setting of security parameters, file protections and enabling of audit logging in proportion to the importance, sensitivity, and accountability requirements of the data processed by the system.
 - Disabling or changing of passwords associated with default accounts.
 - Installation of appropriate intrusion detection and/or file integrity software.
- The Department of Information Technology is responsible for ensuring Lamar State College – Orange systems have been properly specified, configured, installed and continue to be maintained.
- The Department of Information Technology tests security patches before installation where technically feasible.
- The Department of Information Technology must implement security patches in a timely and appropriate manner.
- The Department of Information Technology will periodically examine all systems, in proportion to data sensitivity. System administrators must maintain an inventory of systems, operating system versions in use, critical software and versions that are use, as well as the last time patches were applied. System administrators will also be expected to monitor security mailing lists, and other information sources, for vulnerabilities concerning their operating systems and software

22. Software Licensing

All software used on the Lamar State College - Orange computers will be used in accordance with the applicable software license:

- Lamar State College - Orange will provide a sufficient number of cost-effective, licensed copies of core business software to enable faculty and staff to perform their work in an expedient and effective manner.
- Department of Information Technology personnel have the right to remove software from Lamar State College - Orange computers for cause. For example, if a user is unable to show proof of license, or if the software is not required for college business purposes and causes problems on the college owned computer.
- The Department of Information Technology maintains records of software purchased by the college and ensures that the installation of the software complies with the license agreement of the software. For audit purposes, a record showing proof of purchase and/or original installation media for each software is retained by the Department of Information Technology.

23. Enterprise Development and Deployment

The protection of Information Resources (including data confidentiality, integrity, and accessibility) must be considered during development or purchase of new enterprise computer applications.

- Departments or entities are responsible for developing, maintaining, and participating in quality assurance/project management practices as appropriate for projects of varying scope, cost, and risk.
- The department(s) that requests the development of an application is the owner of that software system. In most cases, the departmental contact designated during the development process is considered a custodian of the system. Likewise, staff or faculty charged with oversight of the technical infrastructure supporting an application are considered custodians of the application.
- Separate production and development environments will be maintained to ensure the security and reliability of the central production system.
- Whenever possible, new development or modifications to a production system will be made first in a development test environment. These changes are thoroughly tested for valid functionality before being released to the central production environment.

24. Vendor Access

Vendors serve an important function in the support of hardware and software and in some cases possibly even the operations of computer networks, servers, and/or applications.

- Vendors must comply with the Information Resources Use Policy found in the LSC-O Administrative Policies and Procedures Manual, when Information Resources are involved, and any Lamar State College – Orange department engaging a vendor must provide the vendor with a copy of this policy and any other procedures they must follow, including, but not limited to:
 - Safety
 - Privacy
 - Security
 - Auditing
 - Software licensing
 - Acceptable Use
- Vendors will adhere to Federal and State laws to which Lamar State College – Orange must adhere.
- Vendors must report all security incidents involving college resources to the Lamar State College - Orange Information Security Office.
- All vendor accounts and maintenance equipment connecting to the Lamar State College - Orange network to access the Internet or outside organizations will remain inactive except when in use for authorized maintenance.
- Vendor accounts providing access to Lamar State College - Orange Information Resources must be uniquely identifiable and passwords must comply with the Lamar State College - Orange password requirements as detailed in the Institutional Procedures Manual for Information Resources.
- Upon departure of a vendor employee from a Lamar State College - Orange contract for any reason, the vendor will ensure that the employee's access to all Lamar State College - Orange sensitive and confidential information is removed within 24 hours in a manner agreed upon by Lamar State College - Orange.
- All software used by the vendor in providing service to Lamar State College – Orange must be properly inventoried and licensed. Software provided by Lamar State College - Orange installed on vendor equipment must be removed at the end of the contract.

25. Disciplinary Actions

Misuse or destruction of Information Resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the severity of the incident. It is not the role of Information Resources Department professionals to carry out disciplinary actions as the result of an incident, but it is their role to monitor resources, to identify potential incidents and to bring such incidents to the

attention of appropriate Lamar State College - Orange executive officials. The following guidelines apply:

- Suspected incidents involving student, faculty, or staff misuse of Information Resources should be brought to the attention of the Information Resources Department.
- If it is determined that a misuse violation has occurred by a student, faculty, or staff member, this should be brought to the attention of the Information Security Office. The Information Security Office will consult with either the Human Resource Services or Student Services, as needed, and in the case of criminal violations, the College Security Department.
- Violations by non-affiliates will be referred to the appropriate authorities.
- Issues of departmental non-compliance may be reported to the respective executive management, the Office of Internal Audit, or the Office of the President.

26. Supporting Documentation

For further details related to Information Resources policies, use, security, and procedures see the following LSC-O internal documents:

- LSC-O Administrative Policies and Procedures Manual
- LSC-O Institutional Procedures for Information Resources

For details related to the policies, use, security, and procedures, for Information Resources that are out-sourced from Lamar University contact the Lamar University - Associate Vice President for Information Technology at 409-880-8493.