1.0 OVERVIEW AND PURPOSE

Technical support staff, security administrators, system administrators, database administrators, network administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program. Intentional or unintentional misuse of these elevated privileges can compromise the university's information security posture.

The purpose of the Lamar University Administrative/Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

2.0 SCOPE

The Lamar University Administrative/Special Access Practice Standard applies equally to all individuals that have, or may require, special access privilege to any Lamar University Information Resources.

3.0 DEFINITIONS

**Information Resources (IR):** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to,

- mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers,
- distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus.
- Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

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

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

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

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

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

Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Vendor: Someone who exchanges goods or services with Lamar University

4.0 POLICY

- User shall not use administrative access for their regular internet activities:
  - Administrative access or root level access or privileged access (power user) provides users with advanced capabilities such as installation and removal of software, change computer system state by adding or deleting system files. While it is convenient for the user account to have administrative access for installing software directly from the Internet, this provides backdoor for malware (viruses, trojans, keyloggers) to exploit and install themselves without the user's knowledge or intervention. Hence the use of administrative privileges must be restricted to installation, update and removal of software and system updates.
  - University staff, faculty or students tasked with performing administrative activity must obtain a separate administrative account. Users with administrative account must be documented within the department and annually with the office of the Chief Information Officer (CIO). All university systems and applications that are capable of authenticating to the domain must be configured to authenticate to the domain and administrative accounts must be provisioned in the domain with approvals from department chair or director and the CIO. Systems that are not capable of authenticating to the domain must be documented and the accounts must be approved by the department chair or director and the CIO. The documentation of approval is subjected to audit by the university’s internal audit department.

- All users must sign the Lamar University Nondisclosure Agreement before access is given to an account with elevated privileges.
- All users of Administrative/Special access accounts must have account management instructions, documentation, information security training, and authorization set defined.
• Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the ISO or CIO. Any such abuse must be immediately reported to the security operations center or to the offices of the CIO & ISO.
• The security operations center under the direction of the CIO and ISO, or LUPD may escalate privilege to any administrative account or reduce privileges to any administrative account to aid in investigation.
• Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
• Each account used for administrative/special access must meet the Lamar University Passphrase Policy.
• The passphrase for an administrator/special access account must change when an individual with the passphrase leaves the department or Lamar University, or upon a change in the vendor personnel assigned to the Lamar University contract.
• Administrative/special access account must never be shared between users.
• All activities using the administrative/special access account must be logged to the extent allowed by the application or system.
• In the case where a system has only one administrator there must be a passphrase escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation. Any such escrow passphrases must be stored in an encrypted format.
• The use of generic accounts such as department admin which needs to be shared for gaining administrative access is prohibited. Instead, all administrative accounts must follow university's naming convention and must be tied to the owner of the account. For instance, user John Doe has a restricted privileged account of jdoe, then, the administrative account for John Doe must be jdoe_admin.
• Special accounts such as LDAP bind or accounts used to integrate application to the university's authentication source must have an administrative contact registered with the security operations center.
• When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
  o must be authorized by the IRM/ISO.
  o must be created with a specific expiration date
  o must be removed when work is completed.

5.0 ENFORCEMENT
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Lamar University Information Resources access privileges, civil, and criminal prosecution.

6.0 RELATED DOCUMENTS
This Security Policy is supported by the following Security Policy Standards.
<table>
<thead>
<tr>
<th>Reference No.</th>
<th>Policy Standard Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IR Security controls must not be bypassed or disabled.</td>
</tr>
<tr>
<td>2</td>
<td>Security awareness of personnel must be continually emphasized, reinforced, updated and validated.</td>
</tr>
<tr>
<td>3</td>
<td>All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.</td>
</tr>
<tr>
<td>4</td>
<td>Passphrases, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management.</td>
</tr>
<tr>
<td>5</td>
<td>Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.</td>
</tr>
<tr>
<td>6</td>
<td>The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management.</td>
</tr>
<tr>
<td>7</td>
<td>Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.</td>
</tr>
<tr>
<td>9</td>
<td>On termination of the relationship with the agency users must surrender all property and IR managed by the agency. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.</td>
</tr>
<tr>
<td>16</td>
<td>Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.</td>
</tr>
<tr>
<td>17</td>
<td>All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.</td>
</tr>
</tbody>
</table>
7.0 REFERENCES

Copyright Act of 1976

Foreign Corrupt Practices Act of 1977

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The State of Texas Information Act

Texas Government Code, Section 441

Texas Administrative Code, Chapter 202

IRM Act, 2054.075(b)

The State of Texas Penal Code, Chapters 33 and 33A

DIR Practices for Protecting Information Resources Assets

DIR Standards Review and Recommendations Publications

8.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every two years

Last Review Date: January 11, 2011

Next Review Date: January 11, 2013

9.0 APPROVAL

J. Simmons  
President, Lamar University  
January 11, 2011  
Date of Approval

Priscilla Parsons  
Chief Information Officer, Lamar University  
January 18, 2011  
Date of Approval
## 10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Approved Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/11/2011</td>
<td>Initial Version</td>
</tr>
</tbody>
</table>