INFORMATION TECHNOLOGY
LAMAR UNIVERSITY

POLICY NAME Administrative/Special Access Policy
POLICY NUMBER 10.01.02
POLICY SECTION Information Technology
EFFECTIVE DATE 1/11/2011

1.0 OVERVIEW AND PURPOSE

Technical support staff, security administrators, system administrators, database administrators, network administrators and others may have special access privilege requirements to accounts compared with typical or everyday users. Since these administrative and special access accounts have a higher level of access, means that the management of these accounts is extremely important to an overall security program. Misuse of these elevated privileges can compromise the Lamar University's information security posture.

The purpose of the Lamar University Administrative/Special Access Policy 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 Policy applies to all individuals that have, or may require, special access privileges to any Lamar University information resource.

3.0 DEFINITIONS

Information Resources (IR): refer to Information Security Program (ISP) for definition.

Information Resources Manager (IRM): Refer to ISP for definition.

Information Security Officer (ISO): Refer to ISP for definition.

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 administrative activities.
    - University staff, faculty or students tasked with performing administrative activities must obtain a separate administrative account. Users with administrative accounts must be documented annually with the user's department and 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 the user's 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 approval documentation is subject to audit by Lamar University's internal audit department.
- If an investigation is forthcoming or underway, users with administrative/special access accounts to related information resources must refrain from abuse of privilege and must only do investigations under the direction of the ISO or CIO. Report any such abuse must be immediately to the security operations center or to the offices of the CIO & ISO.
- The security operations center may escalate privilege to any administrative account or reduce privileges to any administrative account to aid in investigation under the direction of the CIO and ISO, or LUPD.
- Each account used for administrative/special access must comply with the Lamar University Password Standard.
- The password for an administrator/special access account must change when the account owner changes roles or affiliations with Lamar University, or upon a change in a contracted employee with such access.
- 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 password 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 passwords must be stored in an encrypted format.
- Use of generic accounts, such as department admin, for sharing and gaining administrative access, is strictly prohibited. Instead, all administrative accounts must associate with 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 applications to the Lamar University's authentication source must have an administrative contact assigned and registered with the security operations center.
- When special access accounts are needed for internal or external audit, software development, software installation, or other purpose, the account access must be:
    - Authorized by the IRM/ISO,

- Created with a specific expiration date, and
- Removed when the need is fulfilled.

5.0 ENFORCEMENT

Failure to adhere to the provisions of this policy statement may result in:

1. loss of Lamar University Information Resources access privileges;
2. disciplinary action up to and including termination for employees, contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student;
3. civil or criminal prosecution;
4. personal liability for consequences resulting from policy non-compliance;
5. repudiation of the business agreement with third party provider.

6.0 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
Lamar University Information Security Program (ISP)

7.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: August 9, 2017

Next Review Date: August 8, 2020

8.0 APPROVAL

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

Priscilla Parsons — January 18, 2011
Chief Information Officer, Lamar University — **Date of Approval**

9.0 REVISION HISTORY

Revision Number	Approved Date	Description of Changes
1	1/11/2011	Initial Version
2	8/9/2017	Refer to ISP for some definitions. Removed bulleted statements from the Policy section (2, 3, and 6). Clarified statement 4. Changed “passphrase” to “password” throughout document. Replaced Enforcement section with standard language from Policy template. Removed Related Documents section. Added documents to References section. Changed Review Schedule from 2 to 3 years. Renumbered sections.