INFORMATION TECHNOLOGY
LAMAR UNIVERSITY

POLICY NAME	Security Passphrase Policy
POLICY NUMBER	10.02.02
POLICY SECTION	Information Technology
EFFECTIVE DATE	12/10/2009

1.0 OVERVIEW AND PURPOSE

The purpose of the Lamar University Passphrase policy is to establish the rules and standards for the creation, distribution, safeguarding, termination, and reclamation of the Lamar University user authentication mechanisms in accordance with Texas Administrative Code, Rule 202.75(3A), rule 202.70(1).

2.0 SCOPE

The Lamar University Passphrase policy applies equally to all individuals who use any Lamar University information resource.

3.0 DEFINITIONS

Authentication - Authentication is the act of verifying a person's identity as required to secure access to applications, systems or services.

User Authentication Mechanism - Standards, protocols, tools and technologies involved in the authentication process.

Information Resources Manager (IRM)/Chief Information Officer (CIO) - 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 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 executive management for administering the information security functions within the agency. The ISO is the university's internal and external point of contact for all information security matters.

Information Technology Services (ITS) - The Information Technology Services Division of Lamar University.

Password - A string of characters which serves as authentication of a person's identity which may be used to grant or deny access to private or shared data.

Passphrase - A passphrase is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the passphrase the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information such as a birth date, social security number, and so on. The term passphrase will be used for the rest of the document.

Service Account, LDAP Bind Account, Application Account - A user account that is created explicitly to provide a security context for applications or services. Typically, service accounts are provisioned local to system and application accounts are provisioned in the central directory. Bind Accounts are LDAP specific application accounts use for LDAP authentication and query mechanisms.

Generic Accounts - Accounts that are shared and not tied to a specific user.

Default Account - A default account is a user account that is created when the application/appliance is installed/provided by the vendor in "factory install" state.

Default Passphrase - Passphrase used in a default account.

Standard User Accounts - A standard user account lets a person use most of the capabilities of the computer/application/system. When you use a standard account, you can use most programs that are installed on the computer, but you can't install or uninstall software and hardware, delete files that are required for the computer to work, or change settings on the computer that affect other users.

Privileged User Accounts - Is a user account that lets you make changes that will affect other users. E.g. administrators. Privileged user accounts can change security settings, install software and hardware, and access all files on the computer/system/application. Privileged users can also make changes to other user accounts.

Factors of authentication -Factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know - password/passphrase, Personal Identification Number (PIN).
- Something you have - Smartcard, token.
- Something you are - fingerprint, iris scan, voice.
- A combination of factors/multi-factor - Smartcard and a PIN.

4.0 POLICY

1. All passphrases, including initial passphrases, must be constructed and implemented according to Lamar University passphrase standards referenced in this document.

2. All generated passphrases must comply with the standards referenced in this policy. Passphrases, including but not limited to, one time use, temporary accounts, vendor and contractor accounts, must be changed upon first use prior to accessing any information systems.

3. Passphrases must not be shared with anyone and must be treated as confidential.

4. User account passphrases must not be divulged to anyone. Lamar University ITS and Lamar University contractors must not ask for user account passphrases.

5. The use of generic accounts is not allowed. Exceptions to this may be obtained by the approval of the ISO only if an information system or process cannot use a dedicated account and must be documented with the office of CIO.

6. Recording of passphrases by insecure methods is prohibited. Passphrases must not be written down in easily accessible or visible locations.

7. Computing devices must not be left unattended without enabling a passphrase protected screensaver or logging off the device.

8. Users may not circumvent passphrase entry with auto logon, application remembering, embedded scripts or hard coding passphrases into software. Exceptions may be made for specific applications (like automated backups or service accounts) with the approval of the Lamar University ISO. In order for an exception to be approved there must be a procedure to change the passphrases.

9. If the security of a passphrase is compromised, or is in suspicion of compromise, the owner of the passphrase is responsible for changing the passphrase immediately. In addition, the office of the ISO may change the passphrase for a user's account if the passphrase is in suspicion of compromised or is reported to be compromised.

10. In the event passphrases are found or discovered, the following steps must be taken:
    a. Take control of the passphrases and protect them.
    b. Report the discovery to the ISO via Lamar University Service Desk
    c. Transfer the passphrases to an authorized person as directed by the Lamar University ISO.

11. Stored passphrases must be encrypted before storage. In most cases this encryption must be non-reversible ("one-way") and in accordance with the standards referenced in this document. Storing passphrases in a de-cryptable/reversible format is not recommended. However, if the application or service requires the storage of passphrases in a de-cryptable format, please refer to the encryption requirements in the Lamar University passphrase standards. Applications that use storage mechanisms that cannot adhere with the Lamar University passphrase standards must be identified and documented with the office of CIO.

12. Applications or systems that cannot adhere to the university passphrase policy must be identified, documented and must be isolated on the network when feasible. The office of ISO will provide necessary requirements for the isolation of the applications or systems.

13. Information systems that house data classified as confidential, sensitive or regulated may require additional factors of authentication described in the data classification standards.

14. Passphrase history must be kept when possible to prevent the reuse of a passphrase.

15. Administrators must not circumvent the passphrase policy for any reason including ease of use.

16. Passphrase for default accounts must be changed upon first use. Applications where such

accounts cannot be disabled/deleted the changed passphrases must be securely escrowed with the supervisor.

17. Passphrases for application accounts must be generated according to the Lamar University passphrase standards. Exceptions to this may be obtained by the approval of the ISO and recorded with the office of CIO.

18. All personnel assisted passphrase change procedures must include the following:
    a. Validate the user's identity prior to the passphrase change.
    b. The temporary passphrase must be set to a strong passphrase.
    c. The user must change their passphrase at first use.

19. All security tokens issued by Lamar University, used in multi factor authentication must be returned on demand or upon termination of the affiliation with the University.

20. Exceptions to this policy must be requested and documented through the office of the CIO.

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, or

3. Civil or criminal prosecution.

6.0 RELATED DOCUMENTS

1. Lamar University Passphrase Standard.
2. Examples for creating strong passphrase.
3. Texas administrative code (TAC)

7.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every two years

Last Review Date: August 11, 2014

Next Review Date: August 11, 2016

8.0 APPROVAL

Dr. Kenneth Evans — August 11, 2014

President, Lamar University — **Date of Approval**

Priscilla Parsons — August 11, 2014

Chief Information Officer, Lamar University — **Date of Approval**

9.0 REVISION HISTORY

Revision Number	Approved Date	Description of Changes
1	12/10/2009	Initial Version
2	8/11/2014	