INFORMATION TECHNOLOGY
LAMAR UNIVERSITY

POLICY NAME Security Password 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 Security Password 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.

2.0 SCOPE

The Lamar University Security Password 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) - See description in the Information Security Program (ISP).

Information Security Officer (ISO) - See description in the ISP.

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

Password - A string of characters to authenticate a person's identity to grant or deny access to private or shared data. A password not easily guessed and normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is but 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.

Service Account, LDAP Bind Account, Application Account - A user account 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 - User accounts shared and not tied to a specific user.

Default Account - User account created when the application/appliance is installed/provided by the vendor in "factory install" state.

Default Password - Password used in a default account.

Standard User Accounts - User account that 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 - 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, used to authenticate a user. Examples are:

- Something you know - password, 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 passwords, including initial passwords, must be constructed and implemented according to Lamar University Password Standards.

2. Passwords, 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. Passwords must not be divulged to anyone.

4. Passwords must be kept confidential and shall not be written down in easily accessible or visible locations.
5. Lamar University ITS and Lamar University contractors shall not ask for user account passwords.
6. The use of generic accounts is not allowed.
7. Recording of passwords by insecure methods is prohibited.
8. Users must lock or log off computing devices left unattended.
9. If the password is compromised, the owner of the password is responsible for changing the password immediately. In addition, the office of the ISO may change the password for a user's account if the password is reported or suspected to be compromised.
10. In the event passwords are found or discovered, the person discovering the password must follow these steps:
    a. Take control of the passwords and protect them.
    b. Report the discovery to the ISO via Lamar University Service Desk
    c. Transfer the passwords to an authorized person as directed by the Lamar University ISO.

11. Stored passwords must be encrypted prior to storage. The encryption must be in accordance with the Security Password Standards.

12. Applications or systems that cannot adhere to the Lamar University password 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. Password history must be kept when possible to prevent the reuse of a password.

14. All systems must use a password if technically possible.

15. Password for default accounts must be changed upon first use. Applications where such accounts cannot be disabled/deleted the changed passwords must be securely escrowed with the supervisor.

16. Passwords for application accounts must be generated according to the Lamar University password standards.

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

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

19. 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 Password Standard.
2. Texas Administrative Code (TAC)
3. Lamar University Information Security Program

7.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: August 7, 2017 (Final review of this document)

Next Review Date: N/A – This policy will be incorporated into the Identification and Authentication Policy.

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	Review
3	8/7/2017	Changed all references to Passphrase to Password. Removed policy statement [8], references to standards [11, 13] and redundant statements [2, 5, 9, 17]. Reorganized [4] and simplified [1, 3, 6, 7, 15] policy statements.