TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.13 Password Management

First Approved: March 28, 2013
Revised: June 22, 2017
January 23, 2019
Next Scheduled Review: January 23, 2024

Procedure Statement and Reason for Procedure

User authentication is a means to control who has access to an Information Resource system. Controlling access is necessary for any information resource. Access gained by a non-authorized entity can cause loss of confidentiality, integrity, and availability that may result in the loss of revenue, liability, loss of trust, or reputational harm to Texas A&M International University (TAMIU).

Four factors, or a combination of these factors, can be used to authenticate a user. Examples include:

- something you know – password, Personal Identification Number (PIN)
- something you have – token
- something you are – fingerprint; iris scan; voice
- some place you are – on campus; off campus

The purpose of this SAP is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of TAMIU's user authentication mechanisms. This SAP applies equally to all individuals who use any TAMIU Information Resources. This SAP supplements TAMIU Rule 29.01.99.L1, *Information Resources*.

Procedures and Responsibilities

1. Password Guidelines

All TAMIU computing systems require a login authentication process whereby each user is identified and authenticated through a unique user ID and/or account name. Individual password security is the responsibility of each user. Passwords for TAMIU accounts must follow industry standards and meet the following requirements.

1.1 All passwords, including initial passwords, must be constructed and implemented according to the following TAMIU Information Resources rules:

1.1.1 Passwords are considered confidential information. User account passwords must not be shared. OIT will never ask for user account passwords.

1.1.2 User passwords must be at least 16 characters in length. Servers that maintain confidential information and/or those that are mission critical and require administrative user ID's must have passwords that are at least 36 characters in length.

1.1.3 Passwords must include 3 out of the 4 following conditions:

a. alphanumeric lowercase characters (a-z)
b. alphanumeric uppercase characters (A-Z)
c. numbers (0-9)
d. special symbols (e.g., @, !, #)

1.1.4 Passwords must not contain information identifiable with the account owner such as username, social security number, nickname, relatives' names, birth date, UIN, telephone number, TAMIU name or mascot, etc.

1.1.5 Passwords must not be dictionary words or acronyms regardless of language of origin.

1.1.6 Password history must be implemented on systems that support it to prevent users from reusing a password. Passwords must be created in adherence to Section 2 of this SAP.

1.1.7 Minimum password age is 7 days for employee accounts and 3 days for student accounts.

1.1.8 A user account will automatically be locked after 6 failed attempts (within a 30-minute maximum timeframe). Lockout will be reset after 30 minutes.

1.1.9 Passwords shall be protected both in storage and in transit. Temporary passwords that are transmitted for the sole purpose of establishing a new password or changing a password can be excepted from the requirement to encrypt provided it is a one-time transmission and the user changes the password upon first login.

1.1.10 User passwords must be changed no less than every 2 years.

1.1.11 Inactive user accounts (i.e., no logins) will be disabled after 60 days.

1.1.12 Systems or devices that do not support the aforementioned password requirements must have documented appropriate compensating controls in place to protect information based on classification as defined in TAMIU SAP 29.01.99.L1.31, *Information Classification*.

1.2 User access changes must be reported immediately by the department head when job duty changes no longer require such access or upon employment termination.

1.3 If the security of a password is in doubt, the password must be changed immediately. In the event of compromised passwords, a security incident must be reported to the appropriate system administrator(s) and the Information Security Officer (ISO) in accordance with this SAP.

1.4 Forgotten passwords will be replaced and will not be re-issued.

1.5 Users must not circumvent password rules for the sake of ease of use.

1.6 Users cannot circumvent password entry with auto login, application remembering, embedded scripts, or hard-coded passwords within client software. Exceptions may be made for specific applications and/or systems (such as automated backup) with the approval of the Chief Information Officer (CIO) and/or ISO. In order for an exception to be approved, there must be a procedure to change the passwords. Applications and/or systems granted an exception should have other protective controls such as physical access restriction or limited privileges to other systems or networks (e.g., public kiosks).

1.7 Computing devices must not be left unattended without enabling a password-protected screensaver or logging off or locking the device. The device should automatically lock after a maximum of 15 minutes of inactivity.

1.8 If possible, passwords created by users will be checked with a password audit system that follows the established criteria as stated above for the service or system.

1.8.1 Automated password generation applications must use non-predictable generation methods.

1.8.2 Systems that auto-generate passwords for account establishment must require a password change upon entry into the system.

1.9 Passwords and/or combination of usernames and passwords should not be written down (e.g., post-it notes, emails, notepads, etc.)

1.10 OIT Help Desk password change procedures must include the following:

a. Authenticate the user before changing password.
b. Change to a strong, temporary password (see Password Guidelines).
c. The user must change the temporary password at first login.

1.11 In the event passwords are compromised (e.g., compromised through phishing, found on a post-it note, under a keyboard, etc.), the user account will be disabled. The user must change the password and take a security awareness training before the account is reactivated.

2. Creating a Strong Password

2.1 Combine short, unrelated words with numbers or special characters. For example: **eAt42peN**

2.2 Make the password difficulty to guess but easy to remember.

2.3 Substitute numbers or special characters for letters, but do more than just substitute. For example:

- **livefish** – is a bad password.
- **L1veF1sh** – is better and satisfies the rules, but setting a pattern of 1st letter capitalized and i's substituted by 1's is still weak.
- **l!v3f1Sh** – is far better. The capitalization and substitution of characters are not predictable.

Related Statutes, Policies, Regulations, or Rules

TAC 1, Part 10, Chapter 202, Subchapter C – Information Security Standards for Institutions of Higher Education

TAMIU Rule 29.01.99.L1, *Information Resources*

Appendix

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

Contact Office

Office of Information Technology, 956-326-2310