29.02.99.H1.01 Identification and Authentication

Approved: 7/16/2026
Next Scheduled Review: July 2031

Procedure Summary

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 information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or reputation damage to Texas A&M University-Texarkana (A&M Texarkana).

Three 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
- a combination of factors – Token and a PIN

The purpose of this procedure is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of A&M Texarkana's user authentication mechanisms. This procedure emphasizes Multi-Factor Authentication (MFA), stronger passwords and passphrases, risk-based password changes, and reduced reliance on routine age-based password expiration where enhanced authentication controls are in place. This procedure applies equally to all individuals who use any A&M Texarkana Information Resources.

Definitions

Confidential Information: information that is expected from disclosure requirements under the provisions of applicable law, e.g., the Texas Public Information Act.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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): Person 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 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. At A&M Texarkana, the IRM is the CIO.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security functions within the University. The ISO is A&M Texarkana's internal and external point of contact for all information security matters.

Mission Critical Information: Information defined by the University or information resource owner to be essential to the continued operations of the University or department. Unavailability of such information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Office of Information Technology (OIT or IT): The name of the A&M Texarkana department responsible for computers, networking, and data management.

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.

Risk-Based Authentication: An authentication approach that applies authentication requirements based on the assessed risk of the account, system, access method, user behavior, data sensitivity, and evidence of compromise or anomalous activity. Risk-based authentication may require additional verification, password reset, account review, or other compensating controls when risk indicators change.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed from 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. 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 about the user such as a birth date, social security number, and so on.

Procedures and Responsibilities

1. AUTHENTICATION RULES

All A&M Texarkana computing systems require a login authentication process whereby each user is identified and authenticated through his or her unique User ID and/or account name.

Access to the network and to applications is based on individual roles, and determination of user access levels is the responsibility of the owners of the information or applications being accessed.

1.1 Multi-Factor Authentication (MFA) is required for University accounts, systems, applications, and information resources that contain, process, store, transmit, or provide access to confidential, sensitive, mission critical, or otherwise protected information, and for any other system or access method designated by the Information Security Officer or Information Resources Manager based on risk.

1.1.1 Information Technology will use Microsoft MFA as the standard University MFA service where technically feasible.

1.1.2 The preferred authentication method is the Microsoft Authenticator application when available to the end user.

1.1.3 Alternative authentication methods, such as SMS text message verification, may be used when supported and approved by Information Technology.

1.1.4 Any "remember me," persistent session, trusted device, or similar MFA bypass or reduced-prompt setting must not exceed five days.

1.1.5 Information owners and custodians must notify Information Technology of any information resource that contains confidential or sensitive information so appropriate MFA protection can be evaluated and implemented.

1.1.6 Information resources identified as containing confidential or sensitive information must be protected by MFA through integration with Microsoft MFA, University single sign-on, VPN, Office 365, or another approved access control that enforces MFA.

1.1.7 MFA exceptions must be documented, justified, reviewed and approved by the Information Security Officer or designee, including periodic review when risk conditions, system ownership, vendor access, or technical capability changes.

1.2 All passwords, including initial passwords, must be constructed and implemented according to the following University IR rules:

1.2.1 Passwords are considered confidential information.

1.2.2 User passwords for accounts protected by Multi-Factor Authentication (MFA) and configured to meet enhanced password requirements shall not be subject to mandatory periodic expiration solely based on password age. Passwords must be changed when there is evidence or reasonable suspicion of compromise, when required by the

Information Security Officer or appropriate system administrator based on risk, or when otherwise necessary to comply with applicable security requirements. Periodic password resets shall continue to be required for legacy, local, or non-MFA systems only when MFA or enhanced password requirements cannot be implemented, until those systems are remediated, replaced, or approved for an alternate compensating control in accordance with applicable Texas A&M University System policies and controls.

1.2.3 Enhanced password requirements must be applied based on account type and system capability as follows:

1.2.3.1 Standard user accounts protected by MFA must use passwords or passphrases that are at least 16 characters in length.

1.2.3.2 Privileged accounts, including administrator, elevated-access, and other accounts with access beyond standard user privileges, must use passwords or passphrases that are at least 20 characters in length.

1.2.3.3 Service accounts, system accounts, application accounts, administrative automation accounts, and other non-interactive accounts must use passwords, passphrases, or managed secrets that are at least 32 characters in length unless a shorter length is technically required or an exception is approved by the CISO and DCIO. These accounts must be limited to the access required for their function, stored or managed using approved password or secret management practices, and reviewed when system ownership, vendor access, personnel responsibility, or risk conditions change.

1.2.3.4 Where MFA or the required password length is not available due to technical or operational limitations, the account must comply with applicable system requirements and must be changed at least every 180 days unless an approved exception or compensating control has been documented by the Information Security Officer.

1.2.3.5 Servers that are mission critical and/or contain confidential data must adhere to the applicable MFA, password length, account-type, and risk-based reset requirements for the system capability and account use case.

1.2.4 All passwords must meet 3 out of the 4 following conditions; however, password length, use of passphrases, MFA, and screening against commonly used, expected, or compromised passwords are the primary controls for password strength unless an exception has been requested

and approved by the CISO and DCIO:

1.2.4.1 Alphanumeric lowercase characters (a-z)

1.2.4.2 Alphanumeric uppercase characters (A-Z)

1.2.4.3 Numbers (0-9)

1.2.4.4 Special symbols (e.g., @, !, #)

1.2.5 Passwords must not be anything that can easily be tied back to the account owner such as username, social security number, nickname, relative's names, birth date, UIN, telephone number, University name or mascot, etc.

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

1.2.7 Password history (last 4) must be forced on systems that support it to prevent users from reusing a password. It must be created in adherence to 'Creating a strong password' guidelines at the end of this document.

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

1.2.9 All stored passwords must be encrypted and may never be transmitted as plain text.

1.3 Passwords will be enforced to comply with rule number one of this Procedure. In cases where local accounts or applications do not have this feature, a Procedure will be required to abide with this Procedure.

1.4 Access control changes must be reported immediately when there are job duty changes that no longer require restricted access or upon employment termination.

1.5 User account passwords must not be divulged to anyone. IT will never ask for user account passwords.

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

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

1.8 Administrators must not circumvent Password rules for the sake of ease of use.

1.9 Users cannot circumvent password entries with auto logon, application remembering, embedded scripts, or hardcoded passwords in client software.

This restriction does not prohibit the use of University-approved password managers or secret management tools when used in accordance with University requirements and applicable access controls. Exceptions may be made for specific applications, such as automated backup or approved service processes, with the approval of the University ISO. For an exception to be approved, there must be a documented procedure to protect, review, and change the password or managed secret when risk conditions, system ownership, vendor access, or personnel responsibility change.

1.10 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.

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

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

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

1.12 Password management and automated password generation must be able to maintain auditable transaction logs that contain the following information:

1.12.1 Password change time and date, expiration administrative reset

1.12.2 Action type performed

1.12.3 Source system (e.g., IP and/or MAC address) that originated the change request

1.13 Passwords and/or combination of username and password should not be written via the following methods: post-its, emails, notepads, etc.

1.14 IT Service Desk password change procedures must include the following:

1.14.1 Authenticate the user before changing password.

1.14.2 Change to a strong, temporary password (see password guidelines).

1.14.3 The user must change password at first login.

1.15 In the event passwords are found or discovered, the following steps must be taken:

1.15.1 Take control of the passwords and protect them.

1.15.2 Report the discovery to the IT Service Desk.

1.15.3 Transfer the passwords to an authorized person as directed by the University ISO.

2. CREATING A STRONG PASSWORD

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

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

2.3 Substitute numbers or special characters for letters (But do not just substitute). For example:

2.3.1 livefish – is a bad password

2.3.2 L1veF1sh - is better and satisfies the rules, but setting a pattern of first letter capitalized, and I's substituted by 1's can be guessed.

2.3.3 l!v3f1Sh – is far better. The capitalization and substitution of characters is not predictable.

3. DISCIPLINARY ACTIONS

Violation of this Procedure may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Additionally, individuals are subject to loss of A&M Texarkana Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Tex. Gov't. Code Ch. 2054, Information Resources

Title 1, Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

System Policy 24.01, Risk Management

System Policy 29.01, Information Resources

System Policy 29.02, Information Security

System Policy 29.02.01, Information Security Governance

Texas A&M University System Cybersecurity Standards and Guidelines

Texas A&M System Security Control Standards Catalog

Texas A&M University Texarkana Acceptable Use Policy

NIST 800-63B, Digital Identity Guidelines

Contact Office

Office of Information Technology
903-334-6603

Approved:

Signed by:
Ross Alexander
47C0C20C73FD436...

7/16/2026

Ross C. Alexander, Ph.D.
President, Texas A&M University-Texarkana

Date

Document Revision History

Prior to original publication, this document was numbered 29.01.03.H0.11, *Identification and Authenticiation*

Copies of prior versions are available from Office of Ethics and Compliance

Some content of this procedure was previously included in now obsolete University Procedure 29.01.03.H0.26 *Multi-factor Authentication*