29.01.03.H0.11 Identification and Authentication

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

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 embarrassment to Texas A&M University-Texarkana (hereinafter referred to as University or TAMUT).

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

Reason for Procedure

The purpose of this procedure is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of TAMUT's user authentication mechanisms. This procedure applies equally to all individuals who use any TAMUT 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 TAMUT, 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 TAMUT'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.

Information Technology: The name of the TAMUT 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.

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. PASSWORD RULES

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

1.1.1 Passwords are considered confidential information.

1.1.2 User passwords must be changed at most every 180 days. Servers that are mission critical and/or contain confidential data must also adhere to this requirement.

1.1.3 User passwords must be at least 8 characters in length. Servers that maintain confidential information and/or those that are mission critical and require administrative user IDs must have passwords that are at least 12 characters in length.

1.1.4 Passwords must meet 3 out of the 4 following conditions:

1.1.4.1 Alphanumeric lowercase characters (a-z)

1.1.4.2 Alphanumeric uppercase characters (A-Z)

1.1.4.3 Numbers (0-9)

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

1.1.5 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.

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

1.1.7 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.

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

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

1.2 Passwords will be enforced in order 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 in order to abide with this Procedure.

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

1.4 User account passwords must not be divulged to anyone. INFORMATION TECHNOLOGY will never ask for user account passwords.

1.5 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.

1.6 Forgotten passwords will require a password reset and must be initiated through a technical support request.

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

1.8 Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the University ISO. In order for an exception to be approved, there must be a procedure to change the passwords.

1.9 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.

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

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

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

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

1.11.1 Password change time and date, expiration administrative reset

1.11.2 Action type performed

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

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

1.13 INFORMATION TECHNOLOGY Help Desk password change procedures must include the following:

1.13.1 Authenticate the user before changing password.

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

1.13.3 The user must change password at first login.

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

1.14.1 1Take control of the passwords and protect them.

1.14.2 Report the discovery to the INFORMATION TECHNOLOGY Help Desk.

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

2. DISCIPLINARY ACTIONS

Violation of this SAP 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 TAMUT Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

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

Information Security Officer
903-886-5425