SAP 29.01.03.T0.10 Information Technology Services – Password Authentication

Approved:	May 4, 2006
Revised:	Feburary 27, 2012
Revised:	September 22, 2014
Revised:	December 11, 2017
Next Scheduled Review:	December 11, 2022

Procedure Statement

User authentication is a means to control who has access to an information resource system. Controlling the access is necessary for any information resource. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. This, in turn, may result in loss of revenue, liability, loss of trust, or embarrassment to the university. There are several ways to authenticate a user. Examples are: password, university identification number (UIN), Smartcard, fingerprint, iris scan, or voice recognition.

Reason for Procedure

The purpose of the university password/authentication procedure is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of the university user authentication mechanisms and, in addition, to provide a set of measures that will mitigate information security risks associated with password authentication. Also, there may be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Standard Administrative Procedure (SAP) based on information security risk management decisions and business functions. Such risk management decisions must be documented, reported and approved as an exception by the respective department head and the designated information security officer (ISO). The intended audience is any university employee, staff, faculty, student, guest or visitor that uses information resources requiring authentication.

This SAP applies to all Tarleton State University information resources.

Procedures and Responsibilities

All passwords shall be constructed and implemented according to the following criteria:

1. All passwords shall have passwords that conform to this SAP.

2. Passwords must be treated as confidential information and are classified as such in the data classification standard which is contained under System Regulation 29.01.03.

3. Passwords shall be routinely changedat 365 day intervals for systems processing/storing mission critical and/or confidential data. .

4. Passwords embedded in programs intended for machine-to-machine interaction (e.g. backups, stored procedures) are not subject to the routine change specified above, but instead, system administrators shall have a separate documented process for each respective password, that includes but not exclusive to a compensating control (e.g. an account audit or checkpoint) that ensures a compromised password will not go undetected.

5. Where feasible, owners of systems that maintain mission critical and/or confidential information shall establish a reasonable period of time for passwords to be maintained in history to prevent their reuse.

6. Passwords shall not be anything that can be easily associated with the account owner such as: user name, social security number, UIN, nickname, relative's name, birth date, telephone number, etc.

7. Passwords shall not be dictionary words, repeatable patterns or acronyms regardless of language of origin.

8. Stored passwords shall be encrypted.

9. There shall be a limited number of tries before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated "trial-and-error" attacks on passwords.

10. Changes to access controls must be reported immediately when there has been a change in job duties that no longer require restricted access, or upon termination of employment.

11. If the security of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s).

12. Users should not circumvent password entry with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data. Users should always enter "no" when asked to have a password "remembered".

13. Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device.

14. Forgotten passwords shall be replaced, not reissued.

15. Procedures for setting and changing information resource passwords include the following:
    a. The user must verify his/her identity before the password is changed;
    b. The password must meet Tarleton complexity guidelines and,
    c. The user must change password at first log on – where applicable.

16. Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.

Password management and automated password generation must have the capability to maintain auditable transaction history.

Related Statutes, Policies, or Requirements

Supplements *SAP 29.01.03.T0.19 Security of Electronic Information Resources*

1 Tex. Admin Code Ch. 202, *Information Security Standards*

System Policy 29.01, *Information Resources*

System Regulation 29.01.03, *Information Security*

Definitions

1. **Confidential Information**: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. Further definition of confidential information is contained in System Regulation 29.01.03 data classification standard. Examples of 'confidential data may include but are not limited to:

    - Student information records
    - Medical records
    - Intellectual property as stated in section 51.914 of the Texas Education Code
    - Personally Identifiable Information (PII) such as name in combination with social security number, date of birth or financial account numbers

2. **Information Resources (IR)**: the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

3. **Owner of Information Resources**: an entity responsible for: (1) a business function; and (2) determining controls and access to information resources supporting that business function.

4. **Mission Critical**: information that is defined by the university or information resource owner to be essential to the continued performance of the mission of the university or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical 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.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968.9395