Information Technology Services
Password Authentication
Standard

Approved: February 11, 2020

Standard 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 Standard

The purpose of the university password/authentication standard 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 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 standard applies to all Tarleton State University information resources.

Standards and Responsibilities

1. All passwords shall conform to this standard.

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 changed at 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. 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.

9. 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.

10. 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).

11. 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".

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

13. Forgotten passwords shall be replaced, not reissued.

14. Standards 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.

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

Definitions

Anonymous write capability: the ability of people to save (on Tarleton computers) information they create without their identity being known (to system administrators).

Anonymously originating network traffic: causing a (Tarleton) computer system to send traffic via the network where the custodian/owner is not known.

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

Contact Office

Information Technology Services
CIO of Information Technology Services
254.968.9395