

**Procedure 29.01.03.T1.10 (Effective 5/4/2006)**

(Supplements [Rule 29.01.03.T1](#))

**Information Resources –Password Authentication**

1. GENERAL

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.

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.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all university information resources.

3. PURPOSE

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with password authentication. There may also 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 SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

The intended audience is any university employee, staff, faculty, student, guest or visitor that uses information resources requiring authentication.

4. DEFINITIONS

4.1 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.

4.2 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.

4.3 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.

4.4 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.

## 5. PROCEDURES

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

5.1 Servers that are mission critical and/or maintain confidential information shall have passwords that conform to this SAP.

5.2 Passwords must be treated as confidential information. Passwords shall only be revealed to Tarleton State University Information Resources personnel (e.g., Help desk) if contact has been initiated by end user/system owner; and, such information is absolutely necessary to conduct routine maintenance on information resources.

5.3 Passwords shall be routinely changed (no longer than 120 day intervals for systems processing/storing mission critical and/or confidential data).

5.4 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.

5.5 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.

5.6 Passwords shall not be dictionary words or acronyms regardless of language of origin.

5.7 Stored passwords shall be encrypted.

5.8 There shall be no more than seven tries before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated "trial-and-error" attacks on passwords.

5.9 Changes to access controls on security tokens (e.g., TexanCard) must be reported immediately when there has been a change in job duties which no longer require restricted access, or upon termination of employment.

5.10 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).

5.11 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".

5.11.1 Exceptions may be made for specific applications (like automated backup) with the approval of the information resource owner. In order for an exception to be approved, there must be a procedure in place for the user to change passwords.

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

5.13 Forgotten passwords shall be replaced, not reissued.

5.14 Procedures for setting and changing information resource passwords include the following:

5.14.1 The user must verify his/her identity before the password is changed;

5.14.2 The password must be changed to a “strong” password – (see section 6 below of Password Guidelines); and,

5.14.3 The user must change password at first log on – where applicable.

5.15 Where possible, passwords that are user selected shall be checked by a password audit system that adheres to the established criteria of the system or service.

5.15.1 Automated password generation programs must use non- predictable methods of generation.

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

5.16 Password management and automated password generation must have the capability to maintain auditable transaction logs containing information such as:

5.16.1 Time and date of password change, expiration, administrative reset;

5.16.2 Type of action performed; and,

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

## 6. PASSWORD GUIDELINES

Guidelines for creating a “strong” password:

6.1 Make the password difficult to guess, but easy to remember.

6.2 Passwords should contain:

6.2.1 A mix of upper (A-Z) and lower case (a-z) characters.

6.2.2 At least 2 special characters – as permitted by computing systems (such as !@#%&\*<>).

6.2.3 Numeric characters placed after the first, but before the last, character of the password.

6.3 Substitute numbers or special characters for letters.

6.3.1 For example: “livefish” is a “weak” password; “!1v3f1\$h” is better – i.e., the capitalization and substitution of characters is not predictable.

6.4 Create an acrostic from the first letters of a favorite poem, song, or saying.

6.4.1 For example: “LbP\*H!h\$” is an 8-character password created from “Little Bo Peep has lost her sheep.”

6.5 Passwords should not be easily guessed or “weak.” Avoid choosing passwords that are:

(1) Less than 8 characters long;

(2) Your username;

(3) Names of family, pets, friends, co-workers, etc.;

(4) Words associated with your school, school mascot, etc. (such as, “tarleton” and “texanriders”);

(5) Other personal information easily obtained such as: birthdays, addresses, phone numbers, and license plate numbers;

(6) Word or number patterns (e.g., aaabbb, qwerty, 123321);

(7) Any of the above spelled backwards;

(8) Any of the above preceded or followed by a digit (e.g., secret1, secret);

and,

(9) Certain devices (such as voice mail access from a telephone) require password entry through numeric keypad. In this case, users shall avoid using telephone numbers in any format (5 digit such as 5-3211, 7 digit such as 845-3211 or 10 digit such as 979-845-3211) as the password.

**OFFICE OF RESPONSIBILITY:** Department of Information Resources

**CONTACT:** Executive Director of Information Resources