The Division of Information Technology
University Information Security Standards

Information Security Standard – Password Authentication (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

User authentication is a means to control who has access to information resources. 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. Three factors, or a combination of these factors, can be used to authenticate a user.

Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice
- A combination of factors – Smartcard and a PIN

2. Applicability

This information security standard applies to all University information resources.

The purpose of this information security standard is to provide a set of measures that will mitigate information security risks associated with password and authentication issues. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is based on documented and approved information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

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

3. Definitions

3.1 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.

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is 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.

3.3 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state 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. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.4 Mission Critical Information: 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.

3.5 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.6 User: An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

3.7 Owner of Information Resources: an entity responsible:

(1) for a business function (Department Head); and

(2) determining controls and access to information resources

4. Password Procedures

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

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

4.2 Passwords must be treated as confidential information. Passwords shall only be revealed to West Texas A&M 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.

4.3 Passwords shall be routinely changed (no longer than 180 day intervals for systems processing/storing mission critical and/or confidential data).

4.4 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.

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

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

4.7 Stored passwords shall be encrypted.

4.8 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.

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

4.10 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) and the designated Information Security Officer.

4.11 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".

4.11.1 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.

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

4.13 Forgotten passwords shall be replaced, not reissued.

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

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

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

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

4.15 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.

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

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

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

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

4.16.2 Type of action performed; and,

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

5. Password Guidelines

Guidelines for creating a “strong” password:

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

5.2 Passwords should contain:

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

5.2.2 At least 1 special character – as permitted by computing systems (such as !@#$%^&*<>).

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

5.3 Substitute numbers or special characters for letters.

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

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

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

5.5 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 campus, campus mascot, etc. (such as, “wtamu” and “buffs”);

(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: Information Technology

CONTACT: Chief Information Officer