

**PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE**

29.01.03.P0.08 Information Resources – Password Authentication

Approved May 26, 2009

Revised – February 07, 2011

Next Scheduled Review (February 2012)

1. PURPOSE

- 1.1 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. User authentication is a means to control who has access to an information resource system. Controlling 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, Smartcard, fingerprint, iris scan, or voice recognition.

2. DEFINITIONS

- 2.1 Confidential Information - information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). Examples of "confidential" data may include, but are not limited to:
- 2.1.1 Personally identifiable information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers.
- 2.1.2 Student education records.
- 2.1.3 Intellectual property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code.
- 2.1.4 Medical records.
- 2.2 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.
- 2.3 Owner of information resources – an entity responsible for an operational function and determining controls and access to information resources supporting that function.
- 2.4 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, and failure to comply with regulations or legal obligations, or closure of the University or department.

3. APPLICABILITY AND OFFICIAL RESPONSIBILITIES

- 3.1 This university administrative responsibility applies to all university information resources.
- 3.2 The intended audience is any university faculty member, staff member, student or visitor that uses information resources requiring authentication.
- 3.3 The information resource owner or designee is responsible for ensuring that the risk mitigation measures described in this UAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this UAP. Such risk management decisions must be documented and reported to the Information Security Officer.

4. PROCEDURES

- 4.1 All passwords shall be constructed and implemented according to the following criteria:
 - 4.1.1 Servers that are mission critical and/or maintain confidential information shall have passwords that conform to this UAP.
 - 4.1.2 Passwords must be treated as confidential information.
 - 4.1.3 Passwords shall be routinely changed every 120 days or less.
 - 4.1.4 Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups; stored procedures) are not subject to the routine change specified here. Instead, system administrators shall document a separate risk management process for each such password. This process must include a compensating control (e.g., an account audit) that ensures a compromised password will not go undetected.
 - 4.1.5 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.
 - 4.1.6 Passwords should 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.
 - 4.1.7 Passwords should not be dictionary words or acronyms regardless of language of origin.
 - 4.1.8 Stored passwords shall be encrypted.
 - 4.1.9 Passwords shall never be transmitted as plain text.

- 4.1.10 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.
- 4.1.11 Security tokens (e.g., Smartcard) must be returned when there has been a change in job duties which no longer require restricted access, or upon termination of employment.
- 4.1.12 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).
- 4.1.13 Users shall 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".
 - 4.1.13.1 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 for the user to change passwords.
- 4.1.14 Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device.
- 4.1.15 Forgotten passwords shall be replaced, not reissued.
- 4.1.16 Procedures for setting and changing information resource passwords include the following:
 - 4.1.16.1 The user must verify his/her identity before the password is changed.
 - 4.1.16.2 The password must be changed to a "strong" password – (see section 5 of Password Guidelines below); and,
 - 4.1.16.3 The user must change password at first log on – where applicable.
- 4.1.17 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.
 - 4.1.17.1 Automated password generation programs must use non-predictable methods of generation.
 - 4.1.17.2 Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.

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

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

4.1.18.2 Type of action performed; and,

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

5. PASSWORD GUIDELINES (To create strong passwords)

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 2 special characters – 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." Do not choose passwords that are:

5.5.1 Less than 8 characters long;

5.5.2 Your username;

5.5.3 Names of family, pets, friends, co-workers, etc.;

5.5.4 Words associated with your school, school mascot, etc. (such as, "pvamu" and "panther");

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

- 5.5.6 Word or number patterns (e.g., aaabbb, qwerty, 123321);
- 5.5.7 Any of the above spelled backwards;
- 5.5.8 Any of the above preceded or followed by a digit (e.g., secret1, 1secret); and,
- 5.5.9 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.

Contact Office: Information Security Officer; 936-261-2126