PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.08 Information Resources – Password Authentication
Approved May 26, 2009
Revised February 7, 2011
Revised July 1, 2015
Revised August 14, 2017
Next Scheduled Review: August 2022

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of the Prairie View A&M University (PVAMU) user authentication mechanisms. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

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.

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.

Information Security Officer (ISO) – person responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Official Procedures and Responsibilities

1. GENERAL

1.1 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, increased 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.

1.2 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

2. APPLICABILITY

2.1 This UAP applies to all PVAMU information resources. The intended audience for this UAP includes, but is not limited to, all PVAMU faculty members, staff members, students or visitors that use PVAMU information resources requiring authentication.

3. PROCEDURES

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

3.1.1 Passwords must be treated as confidential information;

3.1.2 Passwords shall be routinely changed every 120 days or less;

3.1.3 Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups; stored procedures) are not subject to the routine change specified here. Service account passwords must be changed with changes in personnel (termination, change in duties, transfer, etc.).

3.1.4 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;

3.1.5 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.;

3.1.6 Passwords should not be dictionary words or acronyms regardless of language of origin and must be unique;

3.1.7 Stored passwords shall be encrypted;

3.1.8 Passwords shall never be transmitted as plain text;

3.1.9 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;

3.1.10 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;

3.1.11 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);

3.1.12 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";

3.1.12.1 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.

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

3.1.14 Forgotten passwords shall be replaced, not reissued;

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

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

3.1.14.1.2 The password must be changed to a "strong" password – (see section 5 of password guidelines below); and,

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

3.1.15 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;

3.1.15.1 Automated password generation programs must use non-predictable methods of generation, should be unique; and,

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

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

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

3.1.16.2 Type of action performed; and,

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

3.2 All servers and workstations shall have passwords that conform to this UAP.

4. PASSWORD GUIDELINES TO CREATE STRONG PASSWORDS

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

4.2 Passwords should contain at least three of the following:

4.2.1 Upper case characters (A-Z);

4.2.2 Lower case characters (a-z);

4.2.3 At least 2 special characters – as permitted by computing systems (such as: !#$%^*<>); and,

4.2.4 Numeric characters.

4.3 Be at least 8 characters long.

4.4 Substitute numbers or special characters for letters.

4.4.1 For example: "livefish" is a "weak" password; "l!v3f1$H" is better – i.e., the capitalization and substitution of characters is not predictable.

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

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

4.6 Passwords should not be easily guessed or "weak." Do not choose passwords that are:

4.6.1 Your username;

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

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

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

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

4.6.6 Any of the above spelled backwards;

4.6.7 Any of the above preceded or followed by a digit (e.g., secret1, 1secret); and,

4.6.8 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.

Related Statutes, Policies, Regulations and Rules

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

The Texas A&M University System Information Security Standards

Security Control Standards Catalog

Contact Office

Office of Information Resources Management	936-261-9350