Information Resources – Password / Authentication

Approved January 20, 2004
Revised November 21, 2006
Revised September 15, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
The scope of this procedure is to manage who has access to an information resource system.

Reason for Standard Administrative Procedure
The purpose of the password/authentication procedure is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of the TEES user authentication mechanisms.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

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

1.1 Password expiration policy:

1.1.1 180 days or less for devices that store confidential information or are considered mission critical

1.1.2 All others must routinely change passwords

1.2 Passwords must be treated as confidential information.

1.3 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.

1.4 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.

1.5 Passwords shall not be dictionary words or acronyms regardless of language of origin.
1.6 Stored passwords shall be hashed.

1.7 Passwords shall never be electronically transmitted as plain text (such as Word, Excel, e-mail, Notepad, etc.).

1.8 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.

1.9 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.

1.10 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).

1.11 Except for kiosk, computing devices shall not be left unattended in unsecured areas without enabling a password protected screensaver or logging off of the device.

1.12 Forgotten passwords shall be replaced, not reissued.

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

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

   1.13.2 The password must be changed to a “strong” password – (see section 1.16 below);

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

1.14 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.

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

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

1.15 Password management and automated password generation must have the capability to maintain auditable transaction logs containing information such as:
1.15.1 Time and date of password change, expiration, administrative reset;

1.15.2 Type of action performed; and,

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

1.16 Where operating systems allow, passwords should contain:

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

1.16.2 At least 1 special character (such as !@#$%^&*<>).

1.16.3 At least 1 numeric character not counting the first and last character of the password.

1.16.4 Minimum of 8 characters

2. EXAMPLES OF STRONG PASSWORDS

2.1 Substitute numbers or special characters for letters.

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

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

2.2.1 For example: “LbP8H!h$” is an 8-character password created from “Little Bo Peep has lost her sheep.”

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

2.3.1 Less than 8 characters long;

2.3.2 Your username;

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

2.3.4 Words associated with your school, school mascot, etc. (such as, “tamu” and “aggie”);

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

2.3.6 Word or number patterns (e.g., aaabbb, qwerty, 123321);
2.3.7 Any of the above spelled backwards;

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

2.3.9 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.

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.14, Information Resources – Password/Authentication

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

Contact Office
Information Technology Services
(979) 847-8585