STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.14 Information Resources – Password-based Authentication

Approved July 18, 2005
Revised July 27, 2006
Revised November 5, 2009
Revised September 15, 2010
Revised August 24, 2013
Revised May 14, 2014
Next scheduled review: May 14, 2019

Standard Administrative Procedure Statement

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 negative impacts such as loss of revenue, liability, loss of trust, or embarrassment to the university.

This Standard Administrative Procedure (SAP) establishes procedures for the creation, distribution, safeguarding and termination of university user password authentication mechanisms.

Definitions

AES - Advanced Encryption Standard

Authentication - verification of the identity of an account owner by validating the correctness of the submitted credential. This is the process of establishing confidence in the identity of users or information systems. There are many ways to authenticate a user. Some examples are password, Smartcard, fingerprint, iris scan, or voice recognition.

Confidential - 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). This includes both confidential data-in-transit and confidential data-at rest.

Examples of "Confidential" data may include, but are not limited to:

- personally identifiable information, such as a Social Security number (SSN) and/or financial account number;
- student education records;
- intellectual property such as certain intellectual property as set forth in Texas Education Code Section 51.914; or
- medical records.

Custodian of an Information Resource - a person responsible for implementing owner-defined controls and access to an information resource. Custodians may include university employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the university and/or the owner.

FIPS – Federal Information Processing Standards

Information Resources - the procedures, computer equipment, computing facilities, software and data which are purchased, designed, built, operated and maintained to collect, record, process, store, retrieve, display, report and transmit information

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

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.

Randomly Generated Password – a password that does not match any recognizable pattern and cannot be easily guessed.

Salt - a salt is a random number of a fixed length that is concatenated (i.e., linked to) to the password before the digest operation. This salt must be different for each stored entry. It must be stored as clear text next to the hashed password.

Official Responsibilities and Procedures

1. APPLICABILITY

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

1.2. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed, e.g., unit heads, system administrators, business partners; and, those individuals who need to be aware of the procedures, e.g., non-technical university employees, staff, faculty, student, guest, or visitor. This SAP also applies to any other entity that uses university information resources that require authentication.

1.3. The information resource owner or designee (e.g., custodian, user) is responsible for ensuring that the risk mitigation measures described in this SAP are implemented.

2. SECURITY

2.1. Passwords must be treated as confidential information.

2.1.1. If the confidentiality of a password is in doubt, the password shall be changed immediately.

2.2. Users must change default or assigned passwords where possible.

2.3. User passwords may 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.

2.4. Passwords should not be a dictionary word or an acronym regardless of language of origin.

2.5. Passwords may not be a repetitive sequence.

2.6. Passwords shall be protected both in storage and in transit.

2.6.1. When passwords are stored, they shall be encrypted using current Federal Information Processing Standards (FIPS) 197 Advanced Encryption Standard (AES) approved algorithms.

2.6.2. Passwords that must be transmitted shall be encrypted.

2.6.3. Temporary passwords that are transmitted for the sole purpose of establishing a new password or changing a password can be excepted from the requirement to encrypt provided it is a one-time transmission and the user must also change the password upon first logon.

2.6.4. Whenever possible, if password hashes are stored instead of plain text passwords, hashes should be:

- current FIPS approved algorithms; and,
- salted; and,
- each salt should be varying across the account population.

2.7. Computing devices shall not be left unattended in unsecured areas without password protecting the information resource (e.g., locking the screen). If possible, a user must enable a password-protected screensaver/lock screen or auto logoff function on potentially unattended computing devices (e.g., mobile devices, office desktop computers).

2.8. The password complexity and expiration policy shall be set by the information resource owner and shall follow one of the procedures in Section 3 "Procedures for Password Complexity and Expiration" of this SAP.

2.9. Forgotten passwords shall be replaced not reissued.

2.10. All university staff should utilize self-service password reset (SSPR) when available.

2.11. If SSPR is not used, and a user requests a password change, the following procedures will be followed:

2.11.1. The identity of the user must be verified before the password is changed (see also SAP *29.01.03.M1.03 Information Resources – Account Management*);

AND

2.11.2. The password must be changed to a temporary password;

AND

2.11.3. The user must change the temporary password at first log on – where applicable.

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

2.13. When automated password generation programs are utilized, non-predictable methods of generation must be employed.

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

2.14. Whenever possible, password management and automated password generation

systems must have the capability to maintain auditable transaction logs containing information such as:

2.14.1. Time and date of password change, expiration, and administrative reset; and,

2.14.2. Type of action performed; and,

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

2.15. If a password has been compromised, the event shall be reported as a security incident in accordance with SAP *29.01.03.M1.09 Information Resources – Crisis Management*.

2.16. Where possible, there shall be no more than seven (7) tries during a short system dependent period (this is dependent upon the system's capability and a documented risk decision by the information resource owner).

2.16.1. Accounts shall be locked for at least 10 minutes or until reviewed by an individual designated by the information resource owner.

2.17. Passwords should be different for each account assigned to one user.

2.18. If a password is not scheduled to expire, and the password is used by a system that keeps track of the number of failed authentications, then such a password expires after 100 failed authentications have been recorded in any one month time frame (reference NIST 800-63, 2011).

3. PROCEDURES FOR PASSWORD COMPLEXITY AND EXPIRATION

The information resource owner shall set the password complexity and expiration policies of the information resource system in accordance with procedures described in this section.

The number and different types of password protected information resources, evolving standards and new threats make it impossible to create a single procedure for password complexity and expiration that fits all devices, identity management systems and situations. As such, the intent of this section is to allow information resource owners flexibility in that information resource owners can trade off password complexity and expiration against measures imposed to limit the number of guesses an adversary can attempt.

The password procedures in this section are influenced by the Electronic Authentication Guide by the National Institute of Standards (NIST 800-63-1).

This SAP aims to meet the "Level-2" security classification set by NIST 800-63-1. That is, for confidential or mission critical data, the maximum probability that, over the life of the

password, an attacker with no *a priori* knowledge of the password will succeed in a password guessing attack is 2^{-14} or 1 in 16,384 attempts. Such an attack assumes the attacker knows the user ID.

In addition to the requirements outlined in Section 2, complexity for passwords used for authentication must meet at least one of the following requirements:

3.1. The password must be a randomly generated password with more than 2^{39} possibilities and must be generated by a password method approved by the University Chief Information Security Officer (CISO@tamu.edu).

These types of passwords are often used for machine-to-machine interactions. This type of password never expires.

OR

3.2. The password must be a passphrase of 16 characters or more. This type of password never expires and is not required to meet the complexity of section 3.5 below.

OR

3.3. The passwords must be part of a multi-factor authentication system. The second factor must be unique to the user and by itself cannot authenticate the user. This type of password never expires.

OR

3.4. The password can only be entered from a physical console (e.g., computer terminal, mobile lock screen, desktop login with remote access disabled). This type of password does not expire.

OR

3.5. If a system or application cannot accommodate the standards stated in section 3.1 through 3.4 above, then, when possible, passwords must be at least eight characters in length and must contain three of the following four groups of characters: lower case letters, upper case letters, symbols or numbers. These passwords must expire after no more than one year.

4. EXCLUSIONS

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 SAP. All exclusions must be in accordance with SAP *29.01.03.M1.27 Exclusions from required Risk Mitigation Measures.*

Related Policies or Requirements

University Rule *29.01.03.M1 Security of Electronic Information Resources*

SAP *29.01.03.M1.03 Information Resources – Account Management*

SAP *29.01.03.M1.09 Information Resources – Crisis Management*

SAP *29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures*

NIST 800-63-1 (2011) Electronic Authentication Guide

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Associate Vice President for Information Technology & Chief Information Officer