Texas A&M University System Standard – Password/Authentication

Standard 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 loss of revenue, liability, loss of trust, or embarrassment to the System Office (SO). There are several ways to authenticate a user. Examples are: password, Smartcard, fingerprint, iris scan, or voice recognition.

Reason for standard

The purpose of the SO password/authentication standard is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of the SO user authentication mechanisms.

Definitions

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). Refer to System Regulation 29.01.03 and the Data Classification Standard for more information.

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

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

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.

Owner of Information Resources - an entity responsible for:

(1) A business function; and

(2) Determining controls and access to information resources supporting that business function.

Mission Critical - information that is defined by the SO or information resource owner to be essential to the continued performance of the mission of the System Office 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 System Office or department.

Official Responsibilities and Standards

1. APPLICABILITY

This Standard (standard) applies to all System Office information resources.

The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with password authentication. There may also be other or additional measures that will provide appropriate mitigation of the risks.

The information resource owner or designee (e.g., custodian, user), is responsible for ensuring that the risk mitigation measures described in this standard 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 standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

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

2. STANDARDS

All passwords shall, be implemented according to the following criteria:

2.1. Passwords must be treated as confidential information.

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

2.3. Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups, stored procedures) are not subject to the routine change specified. 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.

2.4. Where possible, owners of systems that maintain mission critical and/or confidential information shall establish a reasonable method for passwords to be maintained in history to prevent their reuse.

2.5. Stored passwords shall be encrypted.

2.6. Passwords shall never be transmitted as plain text.

2.7. Where possible, there shall be no more than seven tries before a user is locked out of an account.

2.8. If the confidentiality of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall be reported as a security incident in accordance with the standard *Incident Management*.

2.9. Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or auto logoff function.

2.10. Forgotten passwords shall be replaced, not reissued.

2.11. Self-service password reset shall be used when available. When self-service password reset is not available, support staff shall use the following procedures to set and change other users' passwords. These procedures include the following:

2.11.1. The identity of the user must be verified before the password is changed;

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

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

2.12. 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.

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

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

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

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

2.13.2. Type of action performed; and;

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

2.14. 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. Passwords should not be dictionary words or acronyms regardless of language of origin.

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer