Procedure Statement

This Procedure is to provide a set of measures that will mitigate information security risks associated with password and authentication issues.

Reason for Procedure

User authentication is a means to control who has access to information resources. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this PROCEDURE based on documented and approved information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

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:
Something you know – password, Personal Identification Number (PIN)
Something you have – Smartcard
Something you are – fingerprint, iris scan, voice
A combination of the above factors – Smartcard and a PIN

Official Responsibilities / Process

1. Applicability

1.1. This Procedure is intended to apply to all University information resources and those employees, students, guest and/or visitors that use these resources.

1.2. The information resource owner or designee is responsible for ensuring that the risk mitigation measures described in the Procedure are implemented. Based on risk management considerations and business function, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this Procedure. Such risk management decision should be documented and made in consultation with the designated ISO.
2. **Process**

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

2.1. Information Resources that are mission critical and/or maintain confidential information shall have passwords that conform to this Procedure.

2.2. Passwords must be treated as confidential information. Passwords may only be revealed to University Information Resources personnel such as university computer technicians only if such information is absolutely necessary to conduct maintenance on an information resource.

2.3. Passwords with elevated permissions will not be used for day-to-day use.

2.4. Passwords shall be routinely changed (no longer than 90 day intervals for systems processing/storing mission critical and/or confidential data).

2.5. Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups, stored procedures) are not subject to the routine change specified. Instead, owners of systems shall document a separate risk management process for each password. This process must include a compensating control (e.g., an account audit) that ensures a compromised password will not go undetected.

2.6. Where feasible, owners of systems that maintain mission critical and/or confidential information shall not be allowed to reuse the last five (5) passwords. For systems that cannot be configured to meet this criteria, the owner of the system shall establish a reasonable period of time for passwords to be maintained in history to prevent their reuse.

2.7. Passwords should not be anything that can be easily associated with the account owner such as: University name or mascot, user name, social security number, UIN, nickname, relative’s name, birth date, telephone number, etc.

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

2.9. Stored passwords shall be encrypted.

2.10. There shall be no more than five tries before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated “trial-and-error” attacks on passwords.

2.11. Changes to access must be reported immediately to the University ISO or Information Technology Services Management when there has been a change in job duties which no longer require restricted access, or upon termination of employment.

2.12. If the security of a password is in doubt, the password should be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s) and the designated Information Security Officer.
2.13. Discretion should be used when circumventing 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 consider entering “no” when asked to have a password “remembered” for University information resources.

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

2.15. Forgotten passwords shall be reset, not reissued.

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

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

2.16.2. The password must be changed to a “strong” password – (see section 3 below of Password Guidelines); and,

2.16.3. The user will be required to change password at first log on – where applicable.

2.17. 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.

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

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

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

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

2.18.2. Type of action performed; and,

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

Related Statutes, Policies, or Requirements (If applicable)

- TAMU-SA Procedure 29.01.03.O0.01 Electronic Information Services Access and Security
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).

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) - Responsible to the executive management for administering the information security functions within the agency. The ISO is the university’s internal and external point of contact for all information security matters.

Information Resources Manager (IRM) – The IRM ensures that all information resources are acquired appropriately, implemented effectively, and complies with regulations and agency policies. Per requirements of the State of Texas, each agency or institution of higher education must designate an IRM.

Contact Office

- Information Technology Services – (210) 784-4357