Password Procedure

Introduction
User authentication is a means to control who has access to an information resource system. Controlling the access is necessary for any information resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to Texas A&M University-Kingsville (TAMUK).

Purpose
The purpose of this procedure is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the TAMUK user authentication mechanisms.

Audience
This procedure applies to individuals who use any University information resource.

Password Procedure
All passwords must be constructed and implemented according to the following criteria:
1. Passwords must be changed at least every 180 days.
2. Passwords must meet complexity guidelines:
   a. must have a minimum length of eight (8) alphanumeric characters
   b. must contain three of the following:
      i. upper case (A-Z)
      ii. lower case (a-z)
      iii. numeric character (0-9)
   1. should not be at the beginning of the password
   iv. special character (! @ # $ % & * _ + = ? ~ ; : , < > | \ )
      1. cannot be at the end of the password
3. User account passwords must not be divulged or shared with anyone. TAMUK iTech and iTech contractors will not ask for user account passwords.
4. Password history must be kept for three (3) prior iterations to prevent the reuse of a password, if the system is capable.
5. Stored passwords must be encrypted and not transmitted as plain text.
6. There shall be no more than five (5) tries before a user is locked out of an account when the system is capable.
7. If the security of a password is in doubt, the password must be changed immediately.
8. Administrators must not circumvent this Password Procedure for the sake of ease of use.
9. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
10. Self-service password reset shall be used when available.
11. iTech Helpdesk password change procedures must include the following:
    a. authenticate the user to the helpdesk before changing password
    b. the user must change password at first login
12. Users cannot circumvent password entry with auto logon or application remembering.
13. 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 with the Information Security Officer (ISO). This process must include a compensating control (e.g., an account audit) that ensures a compromised password will not go undetected.
14. In the event a password is found or discovered, the following steps must be taken:
   a. Take control of the password and protect it
   b. Report the discovery to the ISO
   c. The password will be changed immediately.

Password Guidelines
1. Passwords must not be easy to guess and they:
   a. should not contain your Username
   b. should not contain your employee number
   c. should not contain your name
   d. should not contain family member names
   e. should not contain nickname
   f. should not contain your social security number
   g. should not contain your birthday
   h. should not contain your license plate number
   i. should not contain your pet's name
   j. should not contain your address
   k. should not contain your phone number
   l. should not contain the name of your town or city
   m. should not contain the name of your department

Disciplinary Actions
Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References
1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441