Password Policy

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.

4. Purpose
The purpose of the Texas A&M University-Kingsville Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Texas A&M University-Kingsville user authentication mechanisms.

5. Audience
The Texas A&M University-Kingsville Password Policy applies equally to all individuals who use any University information resource.

6. Password Policy
6.1. All passwords, including initial passwords, must be constructed and implemented according to the following Texas A&M University-Kingsville
6.2. Password history must be kept to prevent the reuse of a password.
6.3. Stored passwords must be encrypted.
6.4. User account passwords must not be divulged or shared with anyone. Texas A&M University-Kingsville CIS and CIS contractors will not ask for user account passwords.
6.5. If the security of a password is in doubt, the password must be changed immediately.
6.6. Administrators must not circumvent this Password Policy for the sake of ease of use.
6.7. Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Texas A&M University-Kingsville Information Security Officer (ISO). In order for an exception to be approved there must be a procedure to change the passwords.
6.8. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
6.9. CIS Helpdesk password change procedures must include the following:
   6.10.1. authenticate the user to the helpdesk before changing password
   6.10.2. change to a strong password
   6.10.3. the user must change password at first login
6.10. In the event passwords are found or discovered, the following steps must be taken:
   1.1.1. Take control of the passwords and protect them
   1.1.2. Report the discovery to the Texas A&M University-Kingsville Help Desk
   1.1.3. Transfer the passwords to an authorized person as directed by the Texas A&M University-Kingsville ISO

7. Password Guidelines:
7.1. Passwords must be changed at least every 180 days.
7.2. Passwords must have a minimum length of 8 alphanumeric characters
7.3. Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password.
   Special characters should be included in the password where the computing system permits. The special characters are (/@#$%&*_+=?/~`;:,<>|).
7.4. Passwords must not be easy to guess and they:
   7.4.1. must not be your Username
   7.4.2. must not be your employee number
   7.4.3. must not be your name
7.4.4. must not be family member names
7.4.5. must not be your nickname
7.4.6. must not be your social security number
7.4.7. must not be your birthday
7.4.8. must not be your license plate number
7.4.9. must not be your pet's name
7.4.10. must not be your address
7.4.11. must not be your phone number
7.4.12. must not be the name of your town or city
7.4.13. must not be the name of your department
7.4.14. must not be street names
7.4.15. must not be makes or models of vehicles
7.4.16. must not be slang words
7.4.17. must not be obscenities
7.4.18. must not be technical terms
7.4.19. must not be school names, school mascot, or school slogans
7.4.20. must not be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.)
7.4.21. must not be any popular acronyms
7.4.22. must not be words that appear in a dictionary
7.4.23. must not be the reverse of any of the above

7.5. Passwords must not be reused for a period of one year
7.6. Passwords must not be shared with anyone
7.7. Passwords must be treated as confidential information
7.8. Creating a Strong Password
7.9. Combine short, unrelated words with numbers or special characters. For example: eAt42peN
7.10. Make the password difficult to guess but easy to remember
7.11. Substitute numbers or special characters for letters. (But do not just substitute) For example:
   7.11.1. livefish - is a bad password
   7.11.2. L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
   7.11.3. l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable
7.12. A random password generator may be used and can be found on the CIS website found at http://www.cis.tamuk.edu

1. Disciplinary Actions
Violation of this policy 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 Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.