



# PRAIRIE VIEW A&M UNIVERSITY

A Member of the Texas A&M University System

June 16, 2006

OFFICE OF BUSINESS AFFAIRS MEMORANDUM No. FY06-34  
Distributed via Campus Email

TO: Vice Presidents, Deans, Directors and Department Heads

FROM: Mary Lee Hodge MLH  
Vice President of Business Affairs

RE: Update to University Administrative Procedures

Please find the following update to the University's Administrative Procedures Manual:

40.15 Password Policy

Please update your manual accordingly and provide copies to staff members as you deem appropriate. An electronic copy will be available on the Business Affairs web page in the Policy Library. If you have any questions regarding this update you may contact me by email at [mlhodge@pvamu.edu](mailto:mlhodge@pvamu.edu) or at extension 2952 or 2953.

xc: Dr. George C. Wright, President

MLH:pgs

# Prairie View A&M University Administrative Procedures Manual

## 40.15 Password Policy

Issued: June 16, 2006

### 1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Prairie View A&M University entire network. As such, all Prairie View A&M University employees (including contractors and vendors with access to Prairie View A&M University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### 2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

### 3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Prairie View A&M University facility, has access to the Prairie View A&M University network, or stores any non-public Prairie View A&M University information.

### 4.0 Policy

#### 4.1 General

1. Passwords and other access codes must be confidential.
2. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at the beginning of each semester.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least at the beginning of each semester. The recommended change interval is every 30 days.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
6. All user-level and system-level passwords must conform to the guidelines described below.
7. All systems should be configured to allow users to change their own passwords where possible, upon demand without third-party involvement.
8. Administrators must not circumvent the password guidelines requirements for the sake of ease of use.
9. Unattended computing devices must be secured from unauthorized access. Physical security options include barriers such as locked doors or security cables.

#### 4.2 Guidelines

##### 1. General Password Construction Guidelines

Strong passwords are required for all Prairie View A&M University issued access accounts. All passwords, including initial passwords, must be constructed, implemented, and maintained according to the following guidelines:

**Prairie View A&M University**  
**Administrative Procedures Manual**

**40.15 Password Policy**

Issued: June 16, 2006

Passwords must contain the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&^\*()\_+|~-=\`{}[]:;'\<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Poor, weak passwords have the following characteristics and must not be used:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Prairie View A&M University", "PVAMU" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

**2. Password Protection Standards**

Do not use the same password for Prairie View A&M University accounts as for other non-Prairie View A&M University access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various Prairie View A&M University access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for access to the PVAMU LAN.

Do not share Prairie View A&M University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Prairie View A&M University information.

Other "Do not's" include:

- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not reveal a password to the boss
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms

**Prairie View A&M University  
Administrative Procedures Manual**

**40.15 Password Policy**

Issued: June 16, 2006

- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, and Microsoft Office).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every semester. The recommended change interval is every 30 days.

If an account or password is suspected to have been compromised, report the incident to the PVAMU IT Help Desk at 2525 and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by PVAMU IT Services or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

**3. Application Development Standards**

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

**4. Use of Passwords for Remote Access Users**

Computers and devices used to access the Prairie View A&M University infrastructure must do so in a manner that preserves the integrity, availability, and confidentiality of Prairie View A&M University information.

Remote access to the Prairie View A&M University network may be made only through approved connection methods.

Access to the Prairie View A&M University infrastructure via remote access is to be controlled using strong password authentication.

**5.0 Enforcement**

Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.