Policy No: 811
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Password Policy

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 Central State University's (CSU) entire network. As such, all CSU personnel (including contractors and vendors with access to Central State systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

POLICY

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Information Security administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- 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).
- All user-level and system-level passwords must conform to the guidelines described below.

PASSWORD CRITERIA

Poor, weak passwords have the following characteristics and shall 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 "<Company Name>", "sanjose", "sanfran" 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)

Strong passwords have the following characteristics and shall be used where applicable:

- 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 a word 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.

NOTE: Do not use any of these examples as passwords!

PASSWORD PROTECTION STANDARDS AND PROHIBITTED ACTIONS

Users shall not use the same password for CSU accounts as for other non-CSU access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various CSU 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 an NT account and a UNIX account.

Users shall not share CSU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential CSU information.

Prohibited activities shall include:

- Revealing a password over the phone.
- Revealing a password in an email message.
- Revealing a password to the boss.
- Talking about a password in front of others.
- Hinting at the format of a password (e.g., "my family name").
- Revealing a password on questionnaires or security forms.
- Sharing a password with family members.

• Revealing 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 Department of Information Technology & Services (ITS).

Do not use the "Remember Password" feature of applications (e.g., Xtender, Outlook, Netscape Messenger).

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 six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to SERVE and change all passwords.

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

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.

USE OF PASSWORDS AND PASSPHRASES FOR REMOTE ACCESS USERS

Access to the CSU Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

PASSPHRASES

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private

key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.