

Password Policy

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 SUNY Stony Brook CS department's entire network. As such, all SUNY Stony Brook CS department users (including students, faculty, staff, guests, contractors and vendors with access to SUNY Stony Brook CS department 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 SUNY Stony Brook CS department facility, has access to the SUNY Stony Brook CS department network, or stores any non-public SUNY Stony Brook CS department information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a bi-annual basis.
- All production system-level passwords must be part of the CS department systems staff administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every nine 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.
- User accounts on production systems and labs within the DMS or on the department web server must have unique passwords from each other.
- 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.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at SUNY Stony Brook CS department. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- 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 "SUNY Stony Brook CS department", "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.

- Simple substitutions of digits for letters. Zero for “o” (oh), numeral 1 (one) for l (ell)
- Bracketing the above with “#” or “!” or similar using non-alphanumeric characters.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have 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 (9 is strongly recommended).
- 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 either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for SUNY Stony Brook CS department accounts as for other non-SUNY Stony Brook CS department access (e.g., personal ISP account, option trading, benefits, Campus, etc.). Don't use the same password for various SUNY Stony Brook CS department access needs. For example, select one password for a research lab systems and a separate password for your office or department production systems. Also, select a separate password to be used for an NT account and a UNIX account. Your password for production systems should never be the same as used to access an Internet Server system (such as a department web server).

Do not share SUNY Stony Brook CS department passwords with anyone, including, spouse, friends administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential SUNY Stony Brook CS department information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers

If someone demands a password, refer them to this document or have them call someone on the systems staff.

Do not use the "Remember Password" feature of applications (e.g., Eudora, 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 nine months (except system-level passwords which must be changed bi-annually). The recommended change interval is every six months.

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

Password cracking or guessing may be performed on a periodic or random basis by CS department systems staff or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it or the account may be disabled.

C. 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 NIS, TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the SUNY Stony Brook CS department Networks via remote access is to be controlled using a public/private key system with a strong passphrase (e.g.: ssh or sftp). Do not use telnet, rlogin, rsh, ftp as your password is transmitted in clear-text over a non-secure link and subject to capture by network monitoring. Refer to the CS department web site for FAQ's on encrypted methods of communicating remotely.

E. 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.

5.0 Enforcement

Any user found to have violated this policy may be subject to disciplinary action.

6.0 Definitions

Terms

Application Administration Account

(e.g., Oracle database administrator, ISSU administrator).

Definitions

Any account that is for the administration of an application

7.0 Revision History