

Rose-Hulman Institute of Technology 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 Rose-Hulman's entire network. As such, all Rose-Hulman employees (including temporary personnel, contractors and vendors with access to Rose-Hulman 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 password 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 Rose-Hulman facility, has access to the Rose-Hulman network through local or remote connectivity, or stores any non-public Rose-Hulman information.

4.0 Policy

The policy attributes listed in section 4.1 below will be implemented and enforced for all network user accounts managed by IAIT.

4.1 General

- All system-level passwords (e.g., root, localmgr, enable, NT admin, application administration accounts, etc.) must be changed on at least an annual basis.
- All user-level network passwords (e.g., email, web, desktop computer, etc.) must be changed on at least an annual basis. The recommended change interval is every six months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" under a UNIX-like operating system, e.g. Linux or "Run As" under Microsoft Windows must have a unique password from all other accounts held by that user.
- A password history of at least 24 previous passwords shall be maintained before a password can be reused.
- A minimum password age of 1 day shall be effective for all passwords.
- A minimum password length of 8 characters shall be required for all passwords.
- An account shall be locked for a period of at least 3 minutes after 50 failed logon attempts. Windows can generate a large number of failed logon attempts when it tries connecting to network file shares so this number is higher might be expected.
- 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 or later).
- All user-level and system-level passwords must conform to the complexity guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Rose-Hulman. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. The guidelines listed below describe how to create a strong password.

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 "Rose", "Hulman", "Rose-Hulman" 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:

- 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 may be written down or stored online, but they should not be stored on or near the computer and if they are stored electronically they must be encrypted. 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 Rose-Hulman accounts as for other, non-Rose-Hulman, accounts (e.g., personal ISP account, option trading, benefits, etc.).

Do not share Rose-Hulman passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Rose-Hulman 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 while on vacation

If someone demands a password, refer them to this document or have them contact the Office of Human Resources.

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

Finally, if you must write passwords down do not store them anywhere in your office. Instead, place a copy in your purse or wallet. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once annually. The recommended change interval is every six months.

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

Password cracking or guessing may be performed on a periodic or random basis by IAIT security personnel. If a password is guessed or cracked during one of these scans, the user will be notified and asked to change it.

C. Application Development Standards

Rose-Hulman 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 Kerberos , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the Rose-Hulman Networks via remote access, e.g. VPN or dial-up, shall be controlled using the user's Institute-issued account.

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

6.0 Definitions

Terms

Definitions

Term	Definition
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator or IIS administrator).
RADIUS	Authentication protocol usually used for remote access. RADIUS stands for Remote Access Dial-In User Service.
X.509	An authentication protocol using the Key Exchange Algorithm.
LDAP	An Internet standard for protocol for accessing directory information. LDAP stands for Lightweight Directory Access Protocol.
SNMP	SNMP is typically used to monitor and/or manage network-attached devices like routers, switches and computers. SNMP is an acronym for the Simple Network Management Protocol.
VPN	A VPN is a technology that creates a secure tunnel through an insecure or untrusted network like the Internet, thus protecting data transmitted back to Rose-Hulman. VPN stands for Virtual Private Network.