Rock Valley College

Password Procedure

RVC Administrative Procedure (2:30.060)

Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of this Procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this Procedure 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 Rock Valley College (RVC) facility, has access to the RVC network, or stores any non-public RVC information.

General Guidelines

1. All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) are recommended to be changed at least every six months. Some systems (e.g., INB) must be changed every three months.
3. User accounts that have system administration privileges must have a unique password from all other accounts held by that user.
4. Passwords must not be emailed to remote users unless the email is encrypted.
5. Passwords must not be written or displayed on or near a desk or computer.
6. All user-level and system-level passwords must conform to the guidelines described below.

General Password Construction Guidelines

Passwords are used for various purposes at RVC. 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:

1. The password contains less than ten characters
2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as:
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, software.
    c. Birthdays and other personal information such as addresses and phone numbers.
    d. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    e. Any of the above spelled backwards.
    f. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

1. Contain both upper- and lower-case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\` {}[]:”;’<>?,./)
3. Are at least ten alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. 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!

Password Protection Standards

Generally, do not use the same password for RVC accounts as for other non-RVC access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various RVC access needs. For example, select one password for the Engineering systems and a separate password for IT (Information Technology) systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share RVC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential RVC 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 store your password anywhere on your desk
- 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 RVC IT Service Desk.

Do not use the "Remember Password" feature of browsers or applications (e.g., Internet Browser, Outlook, Gmail, Hotmail).

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 mobile 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 the IT Service Desk and change all passwords.

Enforcement

The Director of Information Technology shall be responsible for maintaining and updating Password Protection Standards in a manner consistent with industry standards. Further, the Director of Information Technology shall be responsible for ensuring that password update reminders are sent to individuals on an appropriate basis for the system the individual is using.

RVC students thought to be in violation of this procedure will be referred to the student disciplinary procedure.

Employees thought to be in violation will be referred to employee disciplinary procedures consistent with applicable College policies and contractual obligations. All other presumed violators will be handled on a case-by-case basis.

All requests for clarifications or interpretations of this procedure should be directed to the Vice President of Operations/COO.

Implemented: March 2023