GA 38. Password Policy

Title:	Password policy
Policy Number:	GA 38/ 07.18
Effective Date:	July 24, 2018
Issuing Authority:	VP for Development

1. RATIONALE

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 RHU's entire network. As such, all RHU staff, faculty and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The policy is applicable to 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 belongs to RHU, resides at any RHU location, has access to the RHU network, or stores any RHU information.

2. POLICY

All passwords will meet the following criteria:

- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- All user-level passwords (e.g., email, web, servers, applications etc.) must be changed at least every 120 days.
- 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.
- All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used for various purposes at RHU. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every RHU employee should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters

- The password or a subset of 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 "RHU", "state", "university" 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 between 8 and 32 characters
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain at least one number (e.g., 0-9)
- Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
- Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
- Does not contain personal information, names of family, etc.

Passwords should never be written down or stored on-line

Do not use the same password for RHU accounts as for other non-RHU access (e.g., personal ISP account, option trading, benefIT/IS, etc.). Do not share RHU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential RHU information.

Here is a list of "dont's":

- 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 a supervisor.
- 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.
- Don't reveal a password to vendors.
- In short, don't reveal a password to ANYONE.

- Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger, Internet Explorer, Firefox, Thunderbird).
- 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 proper encryption.
- Change passwords at least once every three months.

Other items to remember:

- If someone demands a password, refer them to this document or have them call the RHU IT/IS Department to determine the validity of their request.
- If an account or password is suspected to have been compromised, report the incident to the RHU IT/IS Department immediately and change all passwords as soon as possible.

3. RELATED DOCUMENTS

> IT Manual

4. APPROVAL AND REVIEW

Approved by RHU Administrative Board on October 22, 2024