Password Policy

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the University network.

2. Purpose

The purpose of these guidelines is to provide best practices for the created of strong passwords.

3. Scope

These guidelines apply to employees, contractors, consultants, temporary and other workers at The American Jewish University, including all personnel affiliated with third parties. These guidelines apply to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, and local router logins.

4. Statement of Guideline

All passwords should meet or exceed the following guidelines

Passwords must have the following characteristics:

- Contain at least 6 alphanumeric characters.
- Must not match any of the last four passwords used

And must contain two of the three following criteria:

- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain six or less characters.
- Single words that can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as usernames, building names, system commands, sites, companies, hardware, or software.

American Jewish University 2015 – All Rights Reserved

- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. Or another example: Take a line from a movie – You Want The Truth? You Can't Handle The Truth and your password will be "Ywtt?Ychtt15"

(NOTE: Do not use either of these examples as passwords!)

5. Policy

5.1 Password Creation

5.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

5.1.2 Users must not use the same password for American Jewish University accounts as for other non-American Jewish University access (for example, personal ISP account, option trading, benefits, and so on).

5.1.3 Where possible, users must not use the same password for various American Jewish University access needs.

5.2 Password Change

5.2.1 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months. The minimum frequency users may change their password is every 30 days.

5.2.2 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

5.3 Password Protection

5.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential **American Jewish University information.** Passwords must not be inserted into email messages, or other forms of electronic communication.

5.3.2 Passwords must not be revealed over the phone to anyone.

5.3.3 Do not reveal a password on questionnaires or security forms.

5.3.4 Do not hint at the format of a password (for example, "my family name").

5.3.5 Do not share American Jewish University passwords with anyone, including

administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

5.3.6 **Do not** write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption. Please contact the Campus Technology Department for recommended encrypted password managers. The master password for any password manager must conform to the Password Construction Guidelines

5.3.7 Do not use the "Remember Password" feature of applications (for example, web browsers).

5.3.8 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

How to change your password on Windows 7 computer (www.aju.edu/HowTo)

5.4 Use of Passwords and Passphrases

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.

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

6. Policy Compliance

6.1 Compliance Measurement

The Campus Technology Department team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus and internal and external audits..

6.2 Exceptions

Any exception to the policy must be approved by the Campus Technology Department team in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.