New Password Requirements

2021-07-26 - Lin Kelly - General

USE A STRONG PASSWORD!

We encourage users to create strong passwords for their DACdb user accounts. In keeping with the trend for better security and stronger passwords, DACdb implemented tighter requirements for acceptable passwords in early 2021. Rotary member IDs no longer meet the acceptable criteria for a strong password. Remember that your password is protecting your personal data - and depending on your security level in DACdb - the personal data of dozens or even thousands of other members. Some helpful tips to create strong passwords:

DO *NOT*:

- Make your *password* the same as your *username*
- Make your password blank
- Make your password "password"
- Make your password your first, last or any combination of your name or partner's name
- Make your DACdb password the same as other passwords used for other services
- Make your password less than twelve (12) characters long
- Share your password with ANYONE else

Requirements:

- Create a password a minimum length of 12 characters long
- Cannot equal your login name
- Must include at least 1 number
- Must include at least 1 lower-case character
- Must include at least 1 upper-case character
- Must include at least 1 special character (%, ^, @, !, etc.)

DO:

- Use a combination of letters (lower and upper case), numbers and special characters (see below)
- Use a password generation tool
- Use a password storage application on your device

Acceptable Characters in Passwords

We encourage users to create strong passwords for their DACdb user accounts. However,

because of the systems we use, there are some 'reserved' characters that if used in a password, may cause login problems in some DACdb systems. Using characters listed as "acceptable" will ensure a better login experience.

Acceptable characters:

a-z
A-Z
0-9
! # $ % & ' * + , . / : ; = ? @ ^ | ~ _ -

Unacceptable Characters:

\ "