Password Management Security Rules

Security rules

The security rules associated with password management are parameters, which are set in place by an organization's IT department to guide users in selecting secure passwords.

Password

A user's (administrative personnel, teaching staff, student, etc.) password constitutes an important parameter in an organization's defense strategy.

Complexity factors

The password must be made up of a certain number of elements such as listed below:

- **Uppercase letter**
- **Lowercase letters**
- **Numbers**
- **Special characters:** (ex.: @, ?, #, $, %, ^, &)

The complexity is respected when the password contains at least three of these four elements.

In order to equip users in creating secure and strong passwords, here are the **minimum standards** to apply in your organization:

Safety rules for students

- Password length: 8 characters
- Number of complexity elements integrated into the password: 3
- Password re-initialization: once per year
- Account locked after 10 unsuccessful attempts
- Password history conservation: 6 last

Safety rules for all staff

- Password length: 8 characters
- Number of complexity elements integrated into the password: 3
- Password re-initialization: 4 times per year
- Account locked after 6 unsuccessful attempts
- Password history conservation: 10 last

Safety rules for privileged accounts

- Password length: 12 characters
- Number of complexity elements integrated into the password: 3
- Password re-initialization: 4 times per year
- Account locked after 3 unsuccessful attempts
- Integration of a multi-factor authenticator (ex.: Microsoft Authenticator, RSA key or token)

A few tips for your users

You must retain (memorize) your password. You must not write it down. Using an encrypted access keychain is a good option. Use a sentence, it's easier to remember! Think of substituting certain characters in your password (ex: change certain letters into numbers and special characters that look similar). Do not use information that would allow you to be identified (ex: your last or first name, your identifier, home address).

Technology tools (for reference purposes)

Password strength tester tool by Kaspersky

Password management software: https://keepass.info/