PASSWORD POLICY

This Policy was approved by the University Board during its 223rd meeting on February 19, 2025

Scope

The scope of this Policy includes anyone with a computer account (staff, instructors, and students) on any system integrated within the *Université Saint-Joseph de Beyrouth* (USJ – Saint Joseph University), hereunder referred to as 'USJ' or 'University', information system that requires a password and has access to internal information.

Roles

CISO (Chief Information Security Officer)
The CISO is responsible for ensuring that all USJ users are abiding by the Password Policy. This means making sure users create strong passwords and update them regularly.

IT Department (STI)
The IT Department is responsible for the implementation of this Policy and its security controls.

Table of Contents

Details

1. Password Creation
The following password guidelines must be configured and enforced to compel users to set up complex passwords:
Every password should:

- Consist of at least 10 characters containing uppercase letters, lowercase letters, special characters, and numbers.
- Differ from the username.
- Differ from the last 3 passwords used.
- Be changed at the first login.
- Exclude sequences of more than 3 identical or consecutive characters (e.g., 111, 123, aaa, etc.).

2. Password Change

- Users must systematically change default passwords as soon as possible.
- Passwords must be changed every 6 months otherwise they will expire.
- The CISO has the right to periodically or randomly perform scanning actions with the aim of cracking passwords. If they manage to disclose or decrypt a password, the concerned user must, as soon as possible, replace it with a new, more complex password in accordance with the relevant procedure.
- Any user suspecting that their password has been compromised must report the incident to the IT Department and the CISO and change all passwords associated with their accounts.

3. Account Lifecycle and Access Rights

- Unused accounts pose a potential security risk and should be promptly deactivated. Regular audits should be conducted to identify and disable accounts that are no longer in use.
- Regular access reviews should be conducted to ensure that the principle of least privilege is maintained. Users should only have access to data and systems necessary for their role, and unnecessary permissions should be revoked.

4. Password Protection

To choose complex passwords, it is strongly advised to:

- Avoid keyboard typing combinations (qwerty, azerty, 123456, etc.).
- Use a unique password for each service. In particular, using the same password for professional email, personal email, or social media is to be avoided.
- Choose a password that is not linked to you (first name, children's names, date of birth, phone number, etc.).
- Never ask a third party to generate a password for you.
- Never disclose your password under any circumstances (IT support, malicious emails, etc.).
- Never share your password with anyone (even colleagues and superiors).
- Ensure that no one watches you enter your password.
- Configure software and browsers so they do not "remember" chosen passwords.
- Avoid writing your passwords in any handwritten or electronic format (papers, files, emails, messaging, etc.). However, you can use a password management tool (Dashlane, LastPass, 1Password, etc.) that centralizes all your passwords in a secure location and helps you choose a complex password. Alternatively, you can keep your passwords in an Excel file protected by a password. This password, in turn, can be compressed into a 7-zip file and protected by a second password.

5. MFA (Multi-Factor Authentication)

- In addition to creating strong and complex passwords, users are required to enable MFA to provide an added layer of security (where possible). This helps protect user accounts even if the password is compromised.
- For enhanced security, it is recommended to use authenticator apps for MFA rather than SMS-based verification, due to the potential vulnerabilities associated with SMS.

6. Methods for Choosing Passwords

There are different methods for choosing complex passwords:

- Phonetic: "I bought 9 CDs at 100 Dollars this afternoon" becomes "Ib9CD@%$tpm"
- First letters : the phrase «*un tiens vaut mieux que deux tu l'auras*» becomes «1tvmQ2tl'A»
- Passphrase: a sentence containing random words, made more complex by the use of character substitutions, uppercase/lowercase letters, and spelling mistakes. For example, "I like car photos." becomes "I1ikeKar!fotoS."

7. Software Development and Platform Administration

Application developers (whether internal or external) and platform administrators ensure that their programs incorporate the following security precautions:

- Applications should only authenticate individual users and not groups.
- Applications should not store passwords in plain text or any easily reversible format.
- Applications should use salting and peppering techniques to enhance password hashing security.
- Applications should not transmit passwords in plain text over the network.
- Applications should implement role management that allows a user to assume another's functions without knowing their password.
- Applications requiring authentication should use Multi-Factor Authentication mechanisms.