PASSWORD POLICY

1. Purpose and scope

1.1. This policy defines the minimum requirements for the creation, use, and management of passwords in the organization.
1.2. It is mandatory for:
a) All staff (employees, interns, collaborators).
b) Suppliers and third parties with access to the organization's systems.
c) User accounts, service accounts, and accounts with administrative privileges.

2. Minimum requirements for user passwords

2.1. Minimum length: **8 characters**.
2.2. Complexity: the password must include at least **3 of the following 4** character groups:
a) Uppercase letters (A–Z).
b) Lowercase letters (a–z).
c) Digits (0–9).
d) Special characters (for example: !, ?, @, #, %, &).

2.3. Restrictions:
a) It must not contain the username or obvious parts of the user's first and/or last name.
b) It must not include obvious personal data (ID number, date of birth, phone number, etc.).
c) Simple dictionary words or predictable patterns (e.g., "12345678", "password", "qwerty", "company2025") are not allowed.

3. Additional requirements for privileged and service accounts

3.1. Minimum length: **12 characters**.
3.2. Complexity: passwords must include **all 4** character groups (uppercase, lowercase, digits, special characters).
3.3. Credentials for these accounts must be managed and stored exclusively in the authorized **corporate password manager**.
3.4. Passwords must be changed when:
a) The user's role or responsibilities change.
b) The user leaves the organization.
c) A contract with a supplier or third party with access to systems ends.

4. Password lifecycle

4.1. The initial password assigned must be changed at the **first login**.
4.2. Maximum password age: passwords must be changed at least every **365 days**, or immediately if compromise is suspected.
4.3. History: re-use of the **last 10 passwords** for the same account is not allowed.
4.4. Lockout due to failed attempts:
a) The account will be locked after **5 consecutive failed login attempts**.
b) Unlocking requires help desk intervention or a strengthened verification procedure (for example, MFA).

5. Password use, storage, and transmission

5.1. Password sharing between individuals is strictly prohibited, including with IT staff.
5.2. It is not allowed to write down passwords on visible paper, sticky notes, unencrypted files, photos on mobile devices, or store them in non-managed browsers.
5.3. Passwords must not be sent in clear text by email, instant messaging, or SMS.
5.4. In systems and applications, passwords must only be stored as **salted secure hashes** (for example, bcrypt or Argon2). The use of obsolete algorithms (MD5, SHA-1, etc.) is expressly forbidden.
5.5. Wherever possible, **multi-factor authentication (MFA)** must be enabled and used in addition to passwords.

6. Password recovery and reset procedures

6.1. Password recovery or reset processes must:
a) Verify the identity of the user using one or more factors (MFA, validated alternative channel, etc.).
b) Log the request and the action taken (audit trail).

6.2. Temporary passwords:
a) Must meet the same minimum length and complexity requirements.
b) Are valid only until the **first login**, at which point the user must define a new permanent password.

7. User responsibilities

7.1. Users are responsible for maintaining the confidentiality of their credentials.
7.2. Users must lock their session or device when leaving their workstation.
7.3. Users must immediately inform the help desk or the security officer of:
a) Any suspicion of misuse of their account.
b) Loss, theft, or possible exposure of their password.

8. Compliance and sanctions

8.1. Non-compliance with this policy may be considered a minor, serious, or very serious offense, in line with applicable internal regulations.
8.2. The organization may apply technical measures (account lockout, access revocation) and disciplinary measures in accordance with applicable law and internal procedures.