INFN Password Policy

CCR_SEC_01
Rev. 01 - 24/08/2025

This document defines the minimum security requirements that must be met when creating and managing user passwords in INFN information systems. Its purpose is to ensure effective protection of user accounts and data, as well as of INFN IT resources.

Where feasible, these requirements shall be enforced and supported by password selection interfaces, to assist users in complying with them.

1. The password used for an INFN account must be different from the passwords used to access external services, such as social media platforms, personal email accounts, commercial platforms, accounts with other institutions, etc.
2. A password is a sequence of characters that must meet the following requirements:
    a. Shall have a minimum length of 10 characters;
    b. Shall contain at least three (3) of the following types of characters:
        i. Lowercase letters: abcdefghijklmnopqrstuvwxyz
        ii. Uppercase letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
        iii. Digits: 0123456789
        iv. Punctuation symbols: ,:;?!
        v. Special characters: -_+*#@^=|\"£$%&/()§°çòàùéèì[]{}€<>
    c. Shall have a maximum validity of 1 year and a minimum validity of 1 day;
    d. Shall be different from the last five (5) passwords used;
    e. Shall not be trivial, such as repetitions of the same character, sequences of adjacent keyboard keys, dictionary words or personal data related to the account;
3. Passwords must never be stored in unencrypted form, whether on electronic or paper media.
4. Credentials for accessing INFN systems are strictly personal: passwords must never be disclosed to anyone.