GUIDELINES ON PASSWORDS

I. OVERVIEW

By definition, "Password" is a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization to a certain ICT resource.

II. AIM

A password provides the following:

- Act as a first line of defense against unauthorized access.
- Safeguard personal, business, or sensitive information.
- Ensure that only the intended users can process a particular resource or data.
- It is important to note that passwords alone as a single form of authentication do not provide sufficient protection to one's digital accounts, thus, it is recommended to use additional authentication factors, such as Time-based One-Time PINs sent via SMS, or generated by software-based authenticators, and hardware-based authenticators like physical keys.

III. STANDARDS FOR PASSWORD REQUIREMENTS

1. ISO/IEC 27002

a. Minimum Requirements / Recommended controls

- No specific complexity requirements outlined.
- Password policy outlining complexity requirements, periodic password resets, and best effort technical controls. Password/authentication best practices should apply.

b. ISO/IEC 27002

- Enforce the use of individual user IDs and passwords to maintain accountability.
- Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors.
- Enforce a choice of quality passwords.
- Force users to change their passwords at the first log-on.
- Enforce regular password changes and as needed.
- Maintain a record of previously used passwords and prevent re-use.
- Not display passwords on the screen when being entered.
- Store password files separately from application system data.
- Store and transmit passwords in protected form.

c. Exact Language / Guidance

- Password management systems shall be interactive and shall ensure quality passwords.

- ISO 27001 Framework[1]
- ISO 27002 Security Policy Template[2]

IV. GOOD PRACTICES FOR DATA SUBJECTS

Section 5.17[3] of the ISO/IEC 27002 standard, "Information security controls"[4] provide guidance to users who can access to and use authentication information should be instructed to comply with the following[5]:

1. Users must maintain the confidentiality of secret authentication information such as passwords and should not share such secret information with anyone else. When multiple users are involved in the use of authentication information or the information is linked to non-personal entities, the authentication information should not be disclosed to unauthorized persons.

2. Users must change their passwords immediately if the confidentiality of their passwords are compromised.

3. Users should select hard-to-guess strong passwords by following industry best practices. For instance:

    - Passwords should not be selected based on personal information that is easy to obtain, such as names or dates of birth.
    - Passwords should not be created based on anything that can be easily guessed.
    - Passwords should not include dictionary words or combinations of these words.
    - Alphanumeric and special characters should be used in the password.
    - There should be a minimum length for passwords.

4. Users should not use the same password for different services.

V. GOOD PRACTICES FOR PICS/PIPS

Section 5.17[6] of the ISO/IEC 27002 standard, "Information security controls"[7] provide guidance on establishment and implementation of organization-wide rules, procedures, and measures for the allocation and management of authentication information.

[1] "Wayback Machine," June 25, 2023, https://web.archive.org/web/20230625050038/https://trofisecurity.com/assets/img/iso27001-2013.pdf.
[2] "Https://Examples.Complianceforge.Com/Example-Written-Information-Secu…," archive.li, April 29, 2021, https://archive.li/bmg7I.
[3] "ISO 27002, Control 5.17, Authentication Information | ISMS.Online," 27.
[4] "ISO/IEC 27002:2022(En), Information Security, Cybersecurity and Privacy Protection — Information Security Controls," accessed October 16, 2023, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en.
[5] "ISO 27002, Control 5.17, Authentication Information | ISMS.Online," https://www.isms.online/, accessed October 16, 2023, https://www.isms.online/iso-27002/control-5-17-authentication-information/.
[6] "ISO 27002, Control 5.17, Authentication Information | ISMS.Online," 27.
[7] "ISO/IEC 27002:2022(En), Information Security, Cybersecurity and Privacy Protection — Information Security Controls," accessed October 16, 2023, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en.

Per the ISO/IEC 27002 standard, PICs/PIPs should comply with the following six requirements for allocation and management of authentication information:

- PICs/PIPs should include the requirements for creation and use of passwords in their employment contracts with their employees.
- When personal passwords or personal identification numbers are generated automatically for enrolment of new users, they should be non-guessable. Furthermore, passwords should be unique to each user and it must be mandatory to change passwords after the first use.
- PICs/PIPs should establish robust procedures to authenticate the identity of a user before he/she is granted a new or replacement authentication information or he/she is provided with temporary information.
- PICs/PIPs should ensure the secure transmission of authentication information to individuals via secure channels and they should not send this information over insecure electronic messages (e.g cleartext).
- Users should confirm the receipt of the authentication information.
- After new IT systems and software programs are installed, PICs/PIPs should change the default authentication information immediately.
- PICs/PIPs should establish and maintain records of all important events related to management and allocation of authentication information. Furthermore, these records should be kept confidential and record-keeping methods should be authorized such as through the use of an approved password tool.