Password Policy

Fusion-IT

February 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Feb 12 2021	Initial document

1 Purpose and Scope

a. The Password Policy describes the procedure to select and securely manage passwords.

b. This policy applies to all regular full-time, regular part-time, temporary, and provisional employees who have an account on any system that resides at any company facility or has access to the company network.

2 Background

a. Within this policy, the following definitions apply:

   i. *Password:* Any memorized secret including passwords, passcodes, passphrases and personal identification number (PIN).

3 Policy

a. *Rotation requirements*

   i. The latest NIST recommendations on memorized secrets discourages the application of periodic password change rules (SP 800-63B Section 5.1.1.2 paragraph 9). However, if a credential is suspected of being compromised, the password in question must be changed immediately and the Information Security Manager (ISM) must be notified at incident@fusion-it.ca.

b. *Password complexity*

   i. User and machine-generated password must:

- Contain at least 10 characters or as many as the system permits it.
- Be composed of alphanumeric characters.
- Avoid using repetitive and sequential characters.
- Avoid using dictionary and context-specific words.
- Not be included in a database of previously (see https://haveibeenpwned.com/Passwords).

c. *Password protection*

   i. Passwords generated by Fusion-IT and communicated to employees must meet the password complexity standard.

   ii. The password of a newly issued personal access and transmitted to an employee must be changed by its recipient within 24 hours of receipt.

   iii. All passwords are treated as confidential information and must not be shared with anyone. If you receive a request to share a password,

deny the request and contact the system owner for assistance in provisioning an individual user account.

iv. Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone. If you must store passwords electronically, do so with a password manager that has been approved by the management. If you truly must share a password, do so through a designated password manager.

v. Set your password manager to automatically log out upon browser close.

vi. Enable multi-factor authentication whenever the system allows it.

vii. Do not use the "Remember Password" feature of applications and web browsers.

viii. If you suspect a password has been compromised, change the password immediately and notify the ISM at incident@fusion-it.ca .

4 Authorship and Approval

Last edit made by Lotana (louis.tant@gmail.com) on Thu, 11 Feb 2021 16:32:34 -0500.

Approved by Lotana (louis.tant@gmail.com) on Thu, 11 Feb 2021 16:32:34 -0500 in commit ebf99becfc2a2578a4ab63779fc654754c492e79.