Password Policy

Fusion-IT

February 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Feb 10 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 employee who have an account on any system that resides at any company facility or has access to the company network.

2 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 should be change immediately and the security incident manager should be notified at incident@fusion-it.ca

b. *Password complexity*

   i. User and machine generated password should:

- Contain at least 10 characters
- Be composed of alphanumeric characters
- Avoid repetitive and sequentials characters (e.g. abc5555)
- Avoid dictonnary and context-specific words (e.g. Fusion.dragon)
- Not be included in a database of previously breached passwords (https://haveibeenpwned.com/Passwords)

   i. Passwords generated by Fusion-IT and communicated to employees should be generated by a random bit generator approved by the management. The should be changed by the employee within 24 hours of reception.

c. *Password protection*

   i. All passwords are treated as confidential information and should not be shared with anyone. If you receive a request toincident share a password, deny the request and contact the system owner for assistance in provisioning an individual user account.

   ii. 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.

iii. The use of multi-factor authentication is required whenever the system allows it.

iv. Do not use the “Remember Password” feature of applications and web browsers.

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

d. Enforcement

i. An employee or contractor found to have violated this policy may be subject to disciplinary action.

3 Authorship and Approval

Last edit made by Lotana (louis.tant@gmail.com) on Wed, 10 Feb 2021 12:28:00 -0500.

Approved by Lotana (louis.tant@gmail.com) on Wed, 10 Feb 2021 12:28:00 -0500 in commit 2f97a2886327a88a28ed4301a80d8aba251af2d8.