Password Policy

XYZ Corporation

January 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jun 1 2018	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 employees, contractors, and any other personnel 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. All system-level passwords should be rotated on at least a quarterly basis. All user-level passwords should be rotated at least every six months.

   ii. If a credential is suspected of being compromised, the password in question should be rotated immediately and the Engineering/Security team should be notified.

b. Password protection

   i. All passwords are treated as confidential information and should 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.

   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 IT. If you truly must share a password, do so through a designated password manager or grant access to an application through a single sign on provider.

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

   iv. If you suspect a password has been compromised, rotate the password immediately and notify engineering/security.

c. Enforcement

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