# Password Policy

My Company

December 2020

## Contents



Table 1: Control satisfaction

| Standard | Controls Satisfied |
|---|---|
| TSC | CC9.9 |

Table 2: Document history

| Date | Comment |
|---|---|
| Dec 23 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 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 and user-level password should be rotated on at least a quarterly basis. All changes must be reflected in MyGlue password manager.

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

   iii. A password must contain at least 16 characters, an upper case and lower case character and a symbol. We recommend using the MyGlue password generator for all you passwords.

   iv. A password cannot contain the user's account name or part of the user's full name that exceed two consecutive characters.

   v. A new password cannot be identical to the last 10 passwords used.

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. Do not use the "Remember Password" feature of applications and web browsers. All passwords must be stored using MyGlue password manager. If you truly must share a password, do so through a MyGlue password manager.

   iii. If you suspect a password has been compromised, rotate the password immediately and notify IT.

a. *Lockout policy*

   i. A maximum of five tries is authorized before getting locked out of a user account.

   ii. A user must wait 30 minutes after five unsuccessful attempts to log in. Alternatively, the IT department can be asked to unlock an account anytime.

b. *Enforcement*

   i. Any exception to the policy must be approved by security management in advance.

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