Password Policy

Privo IT

April 2020

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
November 19, 2019	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. All Employees, including contractors and vendors with access to Privo or its customers' systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their password including but not limited to passwords to user-level accounts, system-level accounts, web accounts, email accounts, screensaver protection, voicemail, and local router logins.

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. All passwords must contain at least 12 characters.

   iii. All passwords must contain both upper and lower case letters.

   iv. All passwords must contain at least one number (0-9).

   v. All passwords must Contain at least one special character *(for example,!$%^& ()_+|~-=‘{}[]:“;’<>?,/).”**

   vi. All passwords must not be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.

   vii. All passwords may not contain personal information such as birth dates, addresses, phone numbers, or names of family members, pets, friends, or fantasy characters.

   viii. All passwords must not contain work-related information such as building names, system commands, sites, companies, hardware, or software.

   ix. All passwords must not contain number or letter patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

   x. All passwords must not contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).

xi. All passwords must Not contain common words with simple substitutions of numbers or special characters for letters (for example, s3cr3t, p@ssw0rd)

xii. All passwords must Not contain any version of "Welcome123" "Password123" "Changeme123" or similar

xiii. 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.

v. Never write down a password. Instead, Employees should try to create passwords that they can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. NOTE: Do not use any example presented here as your password!

vi. Employees must not use the same password for Privo accounts as for other non-Privo accounts.

vii. Employees must not re-use the same password for various Privo accounts.

viii. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

ix. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different

from the passwords used to log in interactively. Where possible SNMP community strings must meet password construction guidelines.

x. Password cracking or guessing may be performed on a periodic or random basis by the IT Security Committee. If a password is guessed or cracked during one of these scans, the user will be required to change it.

xi. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) outside of the LastPass encryption vault.

xii. Any user suspecting that his/her password may have been compromised must report the incident to the Security Committee (security@privoit.com or #security in Slack) and change all passwords.

c. *Enforcement*

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

d. *Customer Password Reset*

i. Any request that is received via email, phone call, SMS, chat etc. to reset a customer's password including but not limited to their network logon, infrastructure components, or other hosted applications must verbally be confirmed with the person making the request before proceeding with the change, even if they called in to the support line. To confirm the identity of the person making the request, a phone call must be made to the phone number on record (mobile or office) for the individual user. If a phone number does not exist on record, a call must be made to the company's HR department to obtain a valid telephone number.

e. *Multi-Factor Authentication*

MFA must be enabled on the following Privo services: i. LastPass i. G-Suite i. VPN i. RDP to Management Server i. Amazon Web Services (AWS) i. ConnectWise IT Glue

a. *Passphrases*

Passphrases generally are used for public/private key authentication. A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example,TheTrafficOnThe101Was*&!$ThisMorning!).