Password Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Nov 28 2024	Updated requirements

1 Purpose and Scope

a. This policy establishes standards for creating, securing, and managing passwords to ensure the protection of systems and sensitive data.

b. This policy applies to all personnel who are responsible for or have access to systems requiring passwords within the CredX network.

2 Policy Overview

a. **Password Rotation and Management**

   i. **System-level passwords** (e.g., root, enable, admin accounts) must be changed immediately upon suspected or confirmed compromise. Mandatory periodic rotation is not required unless compromise is detected, in alignment with NIST SP 800-63B guidance.

   ii. **Service account and privileged passwords** must be rotated at least once every 12 months or immediately upon personnel changes affecting that account.

   iii. **Production system-level passwords and secrets** must be stored in an approved secrets manager. Application secrets, API keys, encryption keys, and signing secrets are held in Heroku Config Vars, separated per environment, rotated regularly, and never committed to source control.

   iv. **User-level passwords** (e.g., email, desktop) must be changed immediately upon suspected compromise. Users may not reuse any of the last five passwords.

   v. **Accounts with back-end, administrative, or privileged access** must have unique passwords distinct from other user accounts.

   vi. **Multi-Factor Authentication (MFA)**: MFA is required for all privileged accounts, production system access, cloud infrastructure access, remote access, and any system containing sensitive or confidential data. MFA must use an approved second factor (authenticator app, hardware token, or equivalent). SMS-based MFA is discouraged and may only be used where stronger options are unavailable.

   vii. **Password Sharing**: Passwords must never be shared or included in emails or other electronic communications.

b. **Password Requirements**

   i. **Change Frequency**: Passwords must be changed immediately upon suspected or confirmed compromise. Routine annual rotation is not mandated for standard user accounts in line with NIST SP 800-63B; however, all passwords must be changed when compromise is detected.

ii. **Password History**: The last five passwords cannot be reused.

iii. **Minimum Length**: Passwords must be at least 12 characters long.

iv. **Complexity**: Passwords must include a combination of lowercase letters, uppercase letters, numbers, and special characters.

v. **Restrictions**: Passwords must not contain dictionary words, proper names, or the user's ID.

vi. **Password Visibility**: Passwords must not be displayed when entered.

vii. **Account Lockout**: Accounts will be locked after six failed login attempts, with a lockout duration of at least 30 minutes, or until an administrator manually re-enables the account.

viii. **Idle Session Timeout**: Users must re-authenticate after 15 minutes of inactivity.

ix. **Exceptions**: Any exceptions to the password settings require approval from a member of the CredX executive team (Founder & CEO, CTO, or Operations Manager). Critical application settings must be reviewed annually.

c. **Password Deletion**

i. **Unused Passwords**: Any unused passwords must be rotated before deletion.

ii. **Inactive Accounts**: User accounts that are no longer in use should be deleted.

iii. **Employee Transitions**: Upon reassignment, release, or dismissal, employee passwords must be deleted immediately.

iv. **Default Passwords**: Default passwords on all equipment must be changed immediately.

v. **Contractor Accounts**: Contractor accounts must be deleted once no longer necessary for their duties.

d. **Application Development Standards**

i **Individual Authentication**: Applications must authenticate individual users, not groups.

i. **Password Storage**: Passwords must never be stored in plain text or in an easily reversible format.

ii. **Role Management**: Applications must allow users to assume other users' roles without needing their passwords.

iii. **Password Retrieval**: Applications must not allow passwords to be retrieved in their original form.

e. **Remote Access**

   i. Remote access to the CredX network must be secured using a Virtual Private Network (VPN) requiring both a user ID and password, or an advanced authentication method, such as biometrics, tokens, or public key infrastructure (PKI).

f. **Enforcement**

   i. **Compliance Monitoring**: The CredX security team will regularly monitor compliance through audits, system reports, and other methods.

   ii. **Consequences**: Individuals found in violation of this policy may face disciplinary action, including termination.

This policy is designed to ensure strong password practices and the protection of sensitive information across all systems and applications.