Password Rotation and Management Standards

Password Rotation Policy

User passwords expire every 90 days. System prompts password change 7 days before expiration.

Service account passwords rotated annually. Privileged account passwords rotated every 60 days.

Immediate rotation required if compromise suspected.

Password History

Cannot reuse last 10 passwords. System enforces password history.

Prevents cycling through small set of passwords. Encourages use of password manager for unique passwords.

Password Complexity

Minimum 12 characters. Must include: Uppercase, lowercase, numbers, special characters.

No dictionary words, personal information, or common patterns. System validates complexity on password change.

Password Manager Requirement

All employees must use company password manager (1Password). Generates strong random passwords.

Stores passwords securely with encryption. Syncs across devices. Enables unique passwords for each account.

Emergency Password Changes

Change passwords immediately if: Account compromised, password shared, employee terminated with shared knowledge.

Security team can force password reset for all users if widespread compromise suspected.

Service Account Password Rotation

Service accounts require 20+ character randomly generated passwords. Stored in password manager with restricted access.

Rotation coordinated with application owners. Test applications after password change. Document rotation completion.

Privileged Account Passwords

Administrator and root passwords require extra security. Stored in privileged access management (PAM) system.

Check-out/check-in process for privileged password use. Session recording for accountability.

Password Reset Process

Self-service password reset via IT portal. Verify identity with security questions or MFA.

Helpdesk can reset with identity verification. Temporary password must be changed on first login.

Password Sharing Prohibition

Never share passwords. Each person must have unique account.

Use password manager's secure sharing for legitimate sharing needs (team accounts).

Sharing passwords violates policy and may result in disciplinary action.

Password Storage

Store passwords only in approved password manager. Never in: Plain text files, spreadsheets, sticky notes, browser (except password manager extension).

Encrypt any documents containing passwords. Limit access to password repositories.

Third-Party Account Passwords

Use SSO for third-party services when available. For services without SSO, follow same password standards.

Store third-party passwords in password manager. Enable MFA on third-party accounts.

Password Audits

IT conducts periodic password audits. Identifies: Weak passwords, expired passwords, shared accounts, password reuse.

Users notified of password issues. Compliance required within 48 hours.

Compromised Password Response

If password found in breach database, force immediate reset. Notify user of compromise.

Check for unauthorized account activity. Monitor account for suspicious behavior.

Password Training

Annual security training includes password best practices. New employees receive password training during onboarding.

Regular reminders about password security. Phishing simulations test password protection.

Password Exceptions

Exceptions to rotation policy require security team approval. Documented justification required.

Compensating controls may be required (additional monitoring, restricted access).

Exceptions reviewed annually.