Password Security Policy

Password Requirements

Minimum 12 characters including uppercase, lowercase, numbers, and special characters. Avoid common words, personal information, or sequential patterns.

Passwords expire every 90 days. Cannot reuse last 10 passwords. System will prompt you to change password 7 days before expiration.

Password Manager Usage

Use company-provided password manager (1Password) to generate and store passwords. Password manager is required for all employees.

Generate random passwords of 16+ characters for maximum security. Password manager syncs across devices and auto-fills credentials.

Multi-Factor Authentication

MFA is required for all company systems. Use authenticator app (preferred) or SMS for second factor. Hardware tokens available upon request.

Backup MFA codes are provided during setup - store securely. Contact IT immediately if you lose access to MFA device.

Password Storage

Never write passwords down or store in plain text files. Don't save passwords in browsers unless using company password manager.

Don't share passwords via email, Slack, or text message. Use secure sharing features in password manager if needed.

Account Security

Enable MFA on personal accounts used for work (GitHub, AWS, etc.). Use unique passwords for each account - never reuse passwords.

Review account activity regularly for suspicious logins. Enable login notifications where available.

Compromised Passwords

Change password immediately if you suspect compromise. Notify IT security team. Review recent account activity for unauthorized access.

If company data may have been exposed, report as security incident. Don't attempt to investigate yourself.

Password Reset Process

Self-service password reset available through IT portal using security questions or MFA. Helpdesk can reset if self-service fails.

Identity verification required for helpdesk resets. New temporary password must be changed on first login.

Service Account Passwords

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

Service account passwords don't expire but should be rotated annually or when personnel with access leave.

Third-Party Accounts

Use SSO (Single Sign-On) for third-party services when available. For services without SSO, follow same password requirements.

Don't use personal email for work-related third-party accounts. Use company email and password manager.

Password Audits

IT conducts periodic password audits to identify weak or compromised passwords. You'll be notified if your password needs changing.

Comply promptly with password change requests. Repeated non-compliance may result in account suspension.