

Password & Access Policy Template

Baseline rules for how credentials are created, stored, and rotated.

Password Requirements

- ☐ Minimum length and complexity requirements
- ☐ No reused passwords across business accounts
- ☐ No shared logins for individual accounts

Password Management

- ☐ A password manager used company-wide, not personal memory or spreadsheets
- ☐ Password manager access itself protected with strong authentication
- ☐ Shared credentials stored in the password manager's sharing feature, not email or chat

Two-Factor Authentication

- ☐ Required on email, financial accounts, and any system holding sensitive data
- ☐ Required on the password manager itself

Rotation & Review

- ☐ Immediate password changes required after any suspected compromise
- ☐ Access reviewed periodically to confirm people still need what they have

Offboarding Tie-In

All credentials an employee had access to are changed or revoked when they leave, not just their own login.

Employee Responsibilities

- ☐ Never share passwords, even with a trusted coworker
- ☐ Report suspected phishing or compromise immediately, without fear of blame