PASSWORDS / MFA / IDENTITY

Password and MFA Policy

A modern password and multi-factor authentication policy for small businesses that want stronger account security without outdated password rules.

Purpose

This policy sets minimum expectations for passwords, passphrases, multi-factor authentication, password managers, and account recovery.

The goal is to reduce account takeover risk while keeping login practices realistic for employees.

Scope

This policy applies to company accounts, cloud applications, email, administrative accounts, remote access, financial systems, customer systems, vendor portals, and any account used for company work.

Password requirements

Passwords and passphrases must be unique for company accounts. Employees must not reuse passwords from personal accounts, previous employers, breached services, or other company systems.

Passwords should be long enough to resist guessing. The company should prefer long passphrases or password-manager-generated passwords over short complex passwords that users cannot remember.

Recommended minimums:

- 14 characters for ordinary user accounts
- 16 or more characters for administrative accounts
- Longer generated passwords for service accounts where supported

Password changes

Routine forced password changes are not required unless there is a reason to believe the password is compromised. Passwords must be changed when:

- An account may have been phished
- A password was shared
- A password was entered into the wrong site
- A device with saved passwords was lost or compromised
- A vendor or employee with access leaves
- A breach notification indicates risk

Multi-factor authentication

MFA is required for:

- Email
- Remote access
- Administrative accounts
- Financial systems
- Cloud management portals
- Password managers
- Systems containing customer, employee, regulated, or sensitive business data

Where possible, phishing-resistant MFA such as security keys, passkeys, or platform authenticators should be preferred for administrators and high-risk users.

MFA prompt safety

Employees must not approve MFA prompts they did not initiate. Unexpected prompts may indicate that an attacker has the password and is trying to complete login.

Unexpected MFA prompts should be reported promptly.

Password managers

The company should use an approved password manager for shared business credentials, privileged credentials, and unique generated passwords.

Employees should not store company passwords in browser sync tied to personal accounts, spreadsheets, notes apps, email drafts, chat messages, photos, or paper lists left near the workstation.

Shared accounts

Shared accounts should be avoided. When a shared account is unavoidable, access must be controlled through an approved password manager or documented process. Shared account passwords must be changed when a person with access leaves or no longer needs access.

Administrative actions should use named accounts whenever possible so activity can be traced to an individual.

Service accounts and application secrets

Service account passwords, API keys, tokens, private keys, and application secrets must be stored securely. They must not be placed in public repositories, unprotected scripts, email, tickets, chat, screenshots, or desktop files.

Service accounts should use the minimum permissions needed and should be reviewed periodically.

Account recovery

Recovery email addresses, phone numbers, backup codes, and emergency access methods must be owned by the company where possible. A former employee, MSP, or vendor should not control the recovery path for business-critical accounts.

Backup codes must be stored securely and rotated if exposed.

Offboarding

When an employee, contractor, MSP, or vendor no longer needs access, the company must remove or disable accounts, revoke sessions, rotate shared credentials, remove MFA methods, and update recovery information where needed.

Implementation checklist

- Require MFA on email and administrator accounts
- Use a password manager
- Inventory shared accounts
- Remove personal emails from business account recovery
- Rotate credentials after vendor or employee exits
- Disable stale accounts
- Prefer passkeys or security keys for admins
- Train employees not to approve unexpected MFA prompts

Disclaimer

This starter policy is general information, not legal advice. Adapt it to your business, contracts, regulatory obligations, and state law.