MFA Policy Template

A practical, copy-ready baseline for teams. Review with legal, security, and business owners before enforcement.

Version: 2026-05-13

Owner: Security / IT

Use: Copy, adapt, and review before enforcing MFA.

1. Purpose

This policy defines how the company enables, verifies, recovers, and reviews multi-factor authentication for workforce and administrator accounts.

2. Scope

MFA is required for:

- Email, identity provider, source control, cloud infrastructure, financial, CRM, support, and production admin systems.
- Employees, contractors, service owners, and administrators with access to company data.
- Shared or break-glass accounts, where allowed, with documented owners and additional review.

3. Approved Methods

Preferred methods:

- Passkeys or hardware security keys for high-risk accounts.
- Authenticator apps using TOTP where passkeys or security keys are unavailable.
- Platform-issued backup codes stored offline before enforcement.

Restricted methods:

- SMS can be used only as a temporary fallback when stronger methods are unavailable.
- Email-only recovery is not sufficient for administrator accounts.

4. Enrollment Requirements

Before MFA is enforced, each user must:

- Register at least one approved primary method.
- Save official platform backup codes where the platform provides them.
- Confirm recovery email and phone information is current.
- Complete one test login after enrollment.

5. Recovery and Reset

MFA resets must use a documented process:

- Verify identity through an approved channel.
- Require two-person approval for administrator or high-risk accounts.
- Record the requester, approver, reason, system, and timestamp.
- Regenerate backup codes after access is restored.
- Review recent sign-in activity after reset.

6. Exceptions

Exceptions must include:

- Business reason.
- Systems affected.
- Temporary expiration date.
- Compensating controls.
- Owner responsible for review.

7. Review Cadence

Security or IT reviews MFA coverage at least quarterly, including:

- Accounts without MFA.
- Accounts using SMS fallback.
- Recent MFA resets.
- Dormant admin accounts.
- Backup-code and break-glass procedures.

8. Employee Message

MFA protects company and customer accounts, but it also changes recovery. Save backup codes before enforcement, keep device time sync enabled, and contact IT before replacing or wiping an enrolled device.