mfa-account-protection-policy.md

Multi-Factor Authentication (MFA) & Account Protection Policy

Purpose

- Reduce account takeover risk for admin and developer accounts with an enforced multi-factor authentication (MFA) requirement.

Scope

- Applies to all privileged accounts (admins, developers, CI/service accounts with interactive access). Non-privileged user accounts are encouraged but not enforced by this policy.

Policy

- All admin and developer accounts must have MFA enabled (TOTP apps like Authy/Google Authenticator or hardware keys such as YubiKey).
- Any account with access to production systems or user data must use MFA and unique credentials.

Enforcement and Evidence

- Enforcement: daily automated checks run against identity provider (Firebase/Auth) to list accounts missing MFA. Failures create tickets in the monitoring system.
- Evidence artifacts provided: automated-check output (CSV), screenshots of MFA enforcement settings, and a dated log entry showing the enforcement run time.

Exceptions

- Temporary exceptions may be granted only with documented business justification and a time-boxed remediation plan.

Roles & Responsibilities

- Security team: owns enforcement checks, reviews exceptions, and maintains remediation timelines.
- Admins/Developers: must enable MFA and provide proof when requested.

Review cadence

- Quarterly policy review; automated enforcement checks run daily with weekly summaries retained for 90 days.

Contact

- security@autopromote.example (replace with actual team alias before uploading)