Multi-Factor Authentication (MFA) Policy

Purpose:
Tapify enforces multi-factor authentication (MFA) as a mandatory security control to safeguard access to production systems, sensitive data, and critical infrastructure.

Scope:
This policy applies to all employees, contractors, and administrators who access production assets, databases, dashboards, or any system containing sensitive information.

Policy:
1. All users must authenticate using MFA (2FA) before accessing Tapify production assets.
2. MFA methods include time-based one-time passwords (TOTP), hardware security keys, or push notifications via an approved authenticator app.
3. Password-only authentication is strictly prohibited for production systems.
4. Access is restricted based on role-based access control (RBAC) principles, with least-privilege enforced at all times.
5. MFA enforcement is applied at both the application and infrastructure layers, including GitHub, Vercel, Supabase, and cloud services.

Responsibilities:
- Engineering team ensures MFA enforcement in all developer tools and CI/CD pipelines.
- IT/security team monitors compliance and audits MFA logs quarterly.

Enforcement:
Failure to comply with this policy may result in suspension of system access and disciplinary actions up to and including termination of contracts or employment.