# Two-Factor Authentication (2FA) Security Policy

## 1. Purpose

This policy establishes requirements for the use, management, and protection of two-factor authentication (2FA) within the organization to reduce the risk of unauthorized access to business systems.

## 2. Scope

This policy applies to all employees, contractors, vendors, and third parties who access company systems, applications, or data.

## 3. Policy Requirements

### a. 2FA Enforcement

- 2FA is required for all business-critical systems, including email, cloud platforms, VPNs, and administrative accounts.
- Privileged accounts must use phishing-resistant 2FA (e.g., hardware tokens, FIDO2 keys, passkeys).

### b. Approved 2FA Methods

- Primary: Hardware security keys (FIDO2, YubiKey, etc.).
- Secondary: App-based authenticators (Microsoft Authenticator, Authy, Google Authenticator).
- Not Allowed: SMS- or email-based 2FA, except for emergency fallback.

### c. Push Verification Protections

- MFA apps must require number matching or code verification.
- Users must never approve unexpected prompts.

### d. Recovery & Backup

- Employees must register at least two 2FA methods (e.g., one hardware key + one authenticator app).
- Recovery codes must be stored securely (password manager or locked physical storage).

### e. Access Controls

- Conditional access policies must restrict logins by device compliance, location, and time (where applicable).

### f. Employee Training

- Security awareness training will include education on MFA scams, phishing, and push fatigue.

## 4. Compliance & Enforcement

Failure to comply with this policy may result in disciplinary action, loss of system access, or contract termination for third parties.

## Acknowledgment

I acknowledge that I have read, understand, and agree to comply with the Two-Factor Authentication (2FA) Security Policy.

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_