E1 Unico Corporation

Multi-Factor Authentication (MFA) Policy

Effective Date: June 2026 | **Version:** 1.0 | **Classification:** Internal / Regulatory
Policy Owner: Manuel Montemayor Jr., Founder & CEO
Contact: Unico@E1Unico.com | 1 (833) 318-6426 | e1unico.com
BBB Accredited Business

> **Policy Statement:** E1 Unico Corporation mandates phishing-resistant Multi-Factor Authentication (MFA) for all access to systems that store, process, or transmit consumer financial data. MFA is enforced at the infrastructure, application, and administrative levels — no single-factor access is permitted for any critical system. This policy applies to all human administrators, developers, and authorized personnel without exception.

1. MFA Requirement Scope

Phishing-resistant MFA is required for all access to the following critical systems:

System	Role	MFA Method	Status
Vercel	Production application hosting & environment secrets	Authenticator app (TOTP) + Passkey / Biometric	✔ Active
Neon (PostgreSQL)	Production database storing all financial data & PII	Authenticator app (TOTP) + Passkey / Biometric	✔ Active
GitHub	Source code repository — enforced org-wide	Authenticator app (TOTP) + Passkey / Biometric	✔ Active
Plaid Dashboard	API key management & financial data access controls	Authenticator app (TOTP)	✔ Active
Stripe Dashboard	Payment processing & financial transaction management	Authenticator app (TOTP) + SMS backup	✔ Active
UnicoOS Admin	Multi-tenant SaaS platform — admin accounts	Password + device-bound session	✔ Active

2. MFA Standards — Phishing Resistance

E1 Unico Corporation enforces phishing-resistant MFA methods that cannot be intercepted or replayed by a phishing attack:

- **Passkeys / Biometrics** — Device-bound authentication using Face ID, Touch ID, or Windows Hello.

Cryptographically tied to the registered device — cannot be phished, cloned, or forwarded.

- **TOTP Authenticator App** — Time-based one-time passwords via Google Authenticator or similar. Short-lived codes (30-second window) that cannot be reused.
- **Hardware Security Keys** — FIDO2/WebAuthn hardware tokens available for highest-risk administrative actions.

Explicitly prohibited: SMS-only MFA is not accepted as a sole second factor for critical system access due to SIM-swap vulnerability. SMS is only permitted as a backup recovery method.

3. Enforcement

- MFA cannot be disabled or bypassed for any critical system account — enforcement is configured at the platform level
- Any team member who loses their MFA device must report it immediately; their account is suspended until MFA is re-enrolled
- New accounts for critical systems are not activated until MFA enrollment is verified
- MFA enrollment is audited quarterly as part of the access review process
- Recovery codes are stored securely offline — never in plaintext or shared via email

4. MFA for Non-Human Systems

Automated and service accounts do not use MFA — instead they use phishing-resistant equivalent controls:

- Short-lived OAuth 2.0 access tokens scoped to minimum required permissions
- TLS 1.3 mutual authentication for all service-to-service API calls
- API keys stored in encrypted environment vaults — never in code or logs
- Automated token rotation enforced — no long-lived static secrets for service accounts

5. MFA Implementation Evidence

The following screenshots document active MFA enrollment across critical systems as of June 2026:

5.1 Vercel — MFA Active

[Screenshot: Vercel Account Settings → Security → Two-Factor Authentication: Enabled]

5.2 GitHub — MFA Active (Organization-wide enforcement)

[Screenshot: GitHub Settings → Password and Authentication → Two-Factor Authentication: Enabled]

5.3 Neon — MFA Active

[Screenshot: Neon Dashboard → Profile → Security → Two-Factor Authentication: Enabled]

5.4 Plaid Dashboard — MFA Active

[Screenshot: Plaid Dashboard → Account Settings → Security → MFA: Enabled]

Policy Approval

This MFA Policy has been reviewed, approved, and is actively enforced across all E1 Unico Corporation critical systems as of the effective date below.

Authorized Signatory	Date	Next Review
Manuel Montemayor Jr., Founder & CEO E1 Unico Corporation		Annual — June 2027